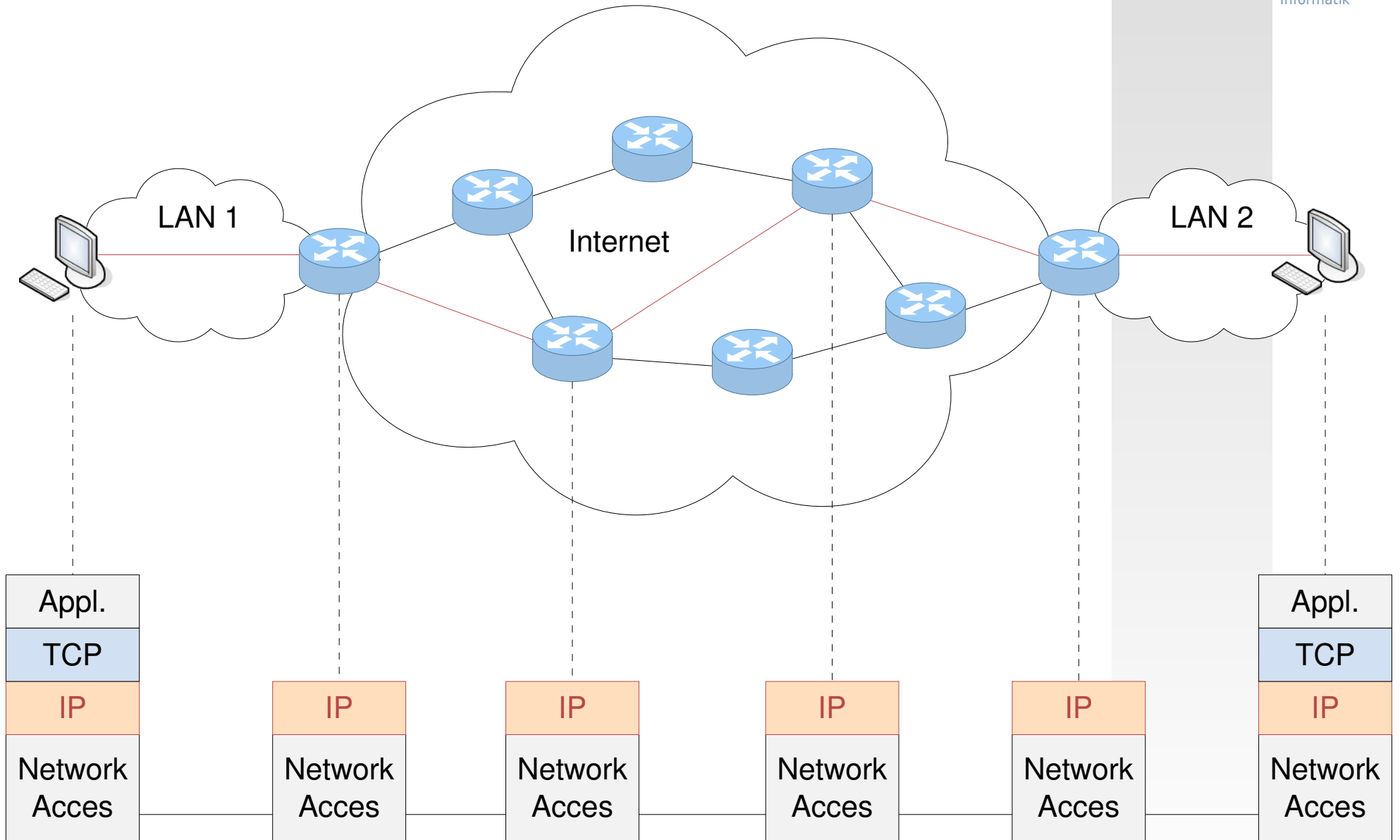
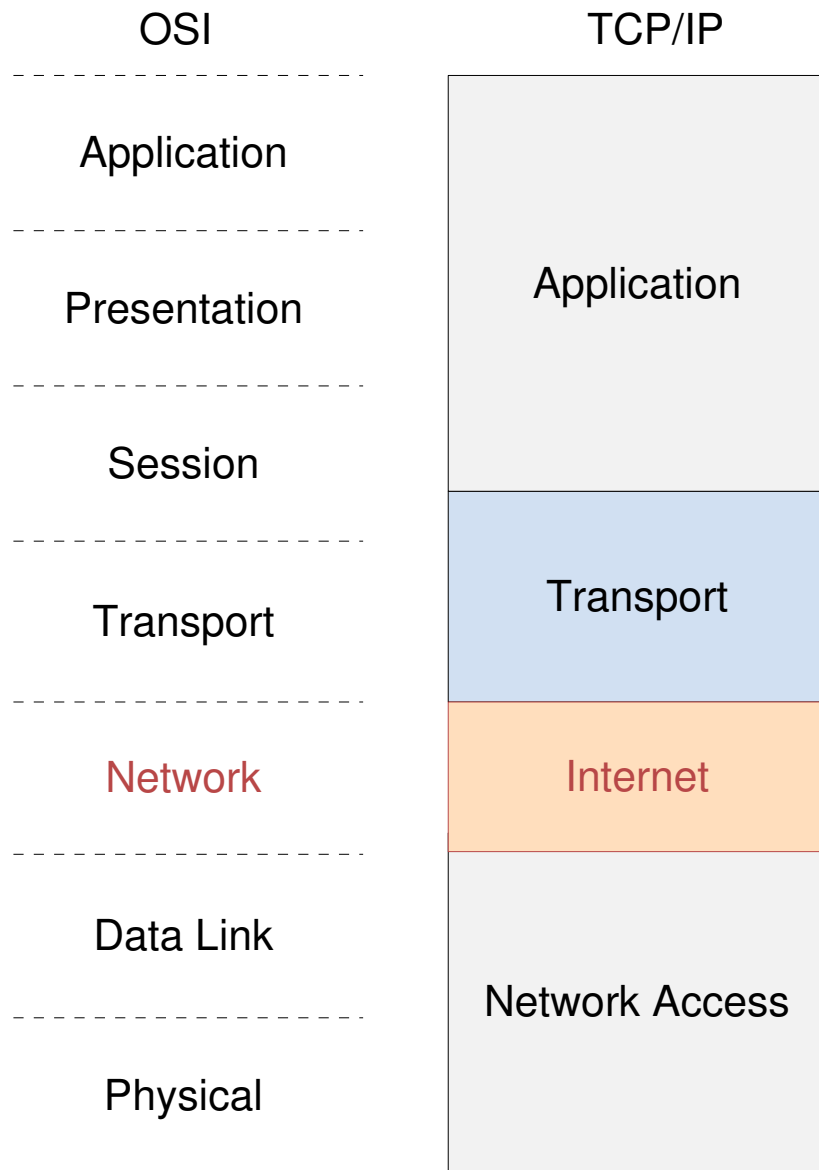


IPv4 - Internet Protocol Version 4

- Einführung
- Paketformat (Datagram)
- Adressierung
- Fragmentierung
- Routing
- Hilfsprotokolle

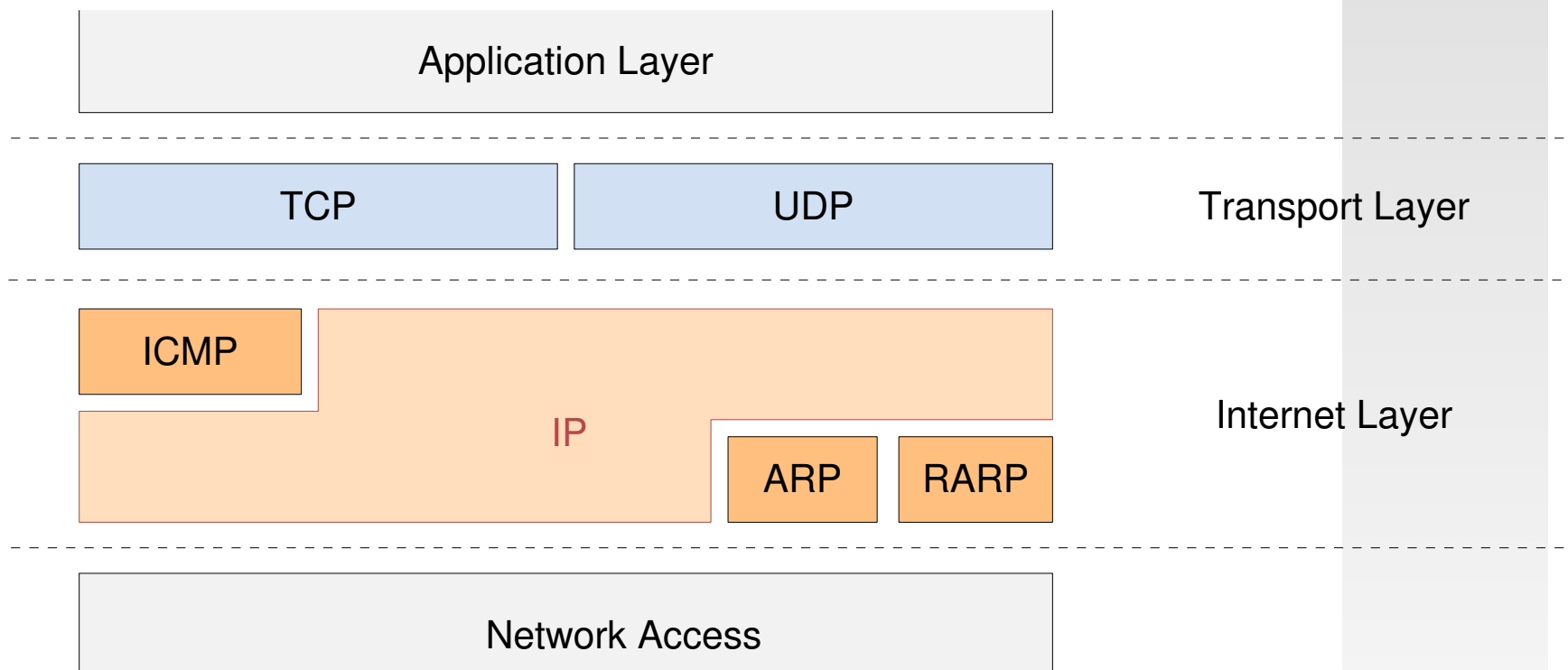
Internet Protocol (IP): Einordnung





- Aufgaben IP (Internet Protocol)
 - Formatierung IP-Datagramme
 - Adressierung
 - Wegwahl (Routing)
 - Fragmentierung
 - Mapping IP- auf MAC-Adressen (ARP)
- Eigenschaften
 - Träger für Transportprotokolle
 - verbindungslos
 - unterschiedliche Wege möglich
 - kein Erhalt der Reihenfolge
 - nicht zuverlässig
- Standard IPv4: RFC 791 (1981)

□ TCP/IP-Protokollstack



IP - Internet Protocol
TCP - Transport Control Protocol
UDP - User Datagram Protocol

ICMP - Internet Control Message Protocol
ARP - Address Resolution Protocol
RARP - Reverse Address Resolution Protocol

□ Implementierungsvorgaben IPv4: RFC 1122

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version				IHL			Type of Service					Total Length																			
Identification												Flags			Fragment Offset																
Time to Live					Protocol					Header Checksum																					
Source Address																															
Destination Address																															
Options																								Padding							
IP Payload (z.B. TCP)																															

- Version
 - 4 – IPv4
 - 6 – IPv6
- Internet Header Length (IHL)
 - Header-Länge in 32-bit-Worten
 - min. 5 (20 Byte), max. 15 (60 Byte)
- Type of Service
 - Dienstanforderungen des Paketes
 - ursprünglich für Quality of Service
- Total Length
 - Gesamtlänge IP-Datagram in Byte
 - max. 65.535

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version				IHL			Type of Service					Total Length																			
Identification											Flags			Fragment Offset																	
Time to Live					Protocol					Header Checksum																					
Source Address																															
Destination Address																															
Options																							Padding								
IP Payload (z.B. TCP)																															

□ Identification:

- eindeutige Identifikation IP-Datagram
- benötigt für Reassembly bei Fragmentierung

□ Flags:

- steuert Fragmentierung

□ Fragmentation Offset:

- Position der Nutzdaten des IP-Datagramms im IP-Paket

□ Time to Live (TTL)

- in jedem Knoten dekrementiert
- wenn 0, wird IP-Datagramm verworfen

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version				IHL			Type of Service					Total Length																			
Identification										Flags			Fragment Offset																		
Time to Live					Protocol					Header Checksum																					
Source Address																															
Destination Address																															
Options																							Padding								
IP Payload (z.B. TCP)																															

□ Source/Destination Address:

- IPv4-Adressen
- Absender bzw. Empfänger

□ Header Checksum:

- Sicherung gegen Übertragungsfehler
- Berechnung nur über Header

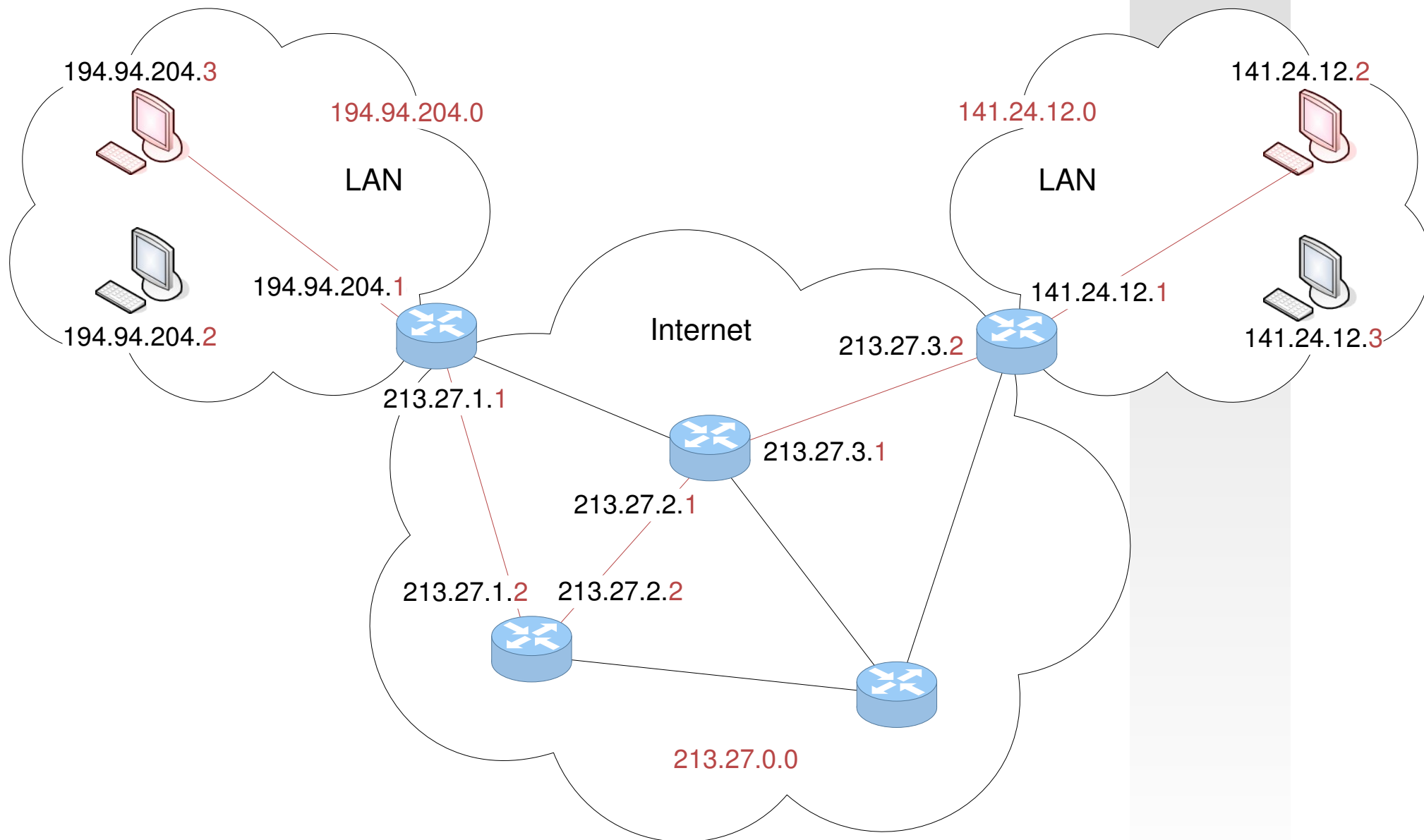
□ Options

- spezielle Informationen (var. Länge)
- max. 40 Byte

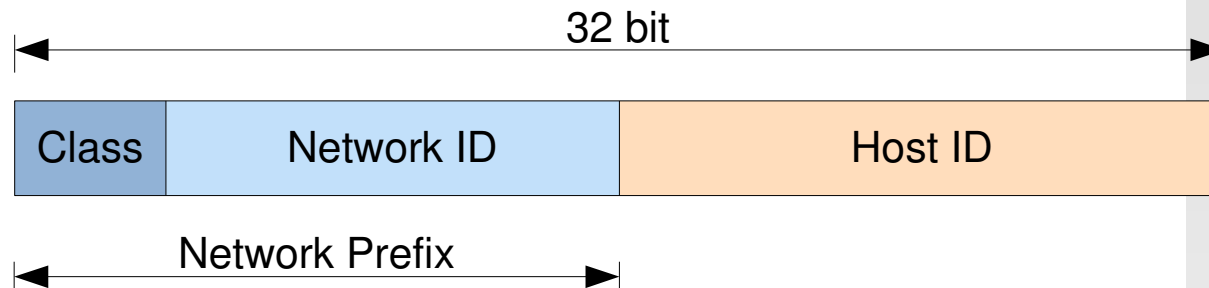
□ Padding:

- Auffüllen Header auf Wortgrenzen
- bei Verwendung von Optionen

IPv4-Adressierung: Problemstellung



□ Adressaufbau (zweistufig)



□ Darstellung (Beispiel)

- binäre Darstellung
- hexadezimale Darstellung
- dezimale Darstellung

Class	Network ID	Host ID
11000001 . 01011110 . 11001100 . 00010111		
C2	5E	CC
194	94	204

□ spezielle Adressen

- **Netzwerkadresse:** Host ID Bits = 0 194.94.204.0
- **Broadcast:** Host ID Bits = 1 194.94.204.255

□ Klassen

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
Class A	0	2 ⁷ Network ID							2 ²⁴ Host ID																												
Class B	1	0	2 ¹⁴ Network ID														2 ¹⁶ Host ID																				
Class C	1	1	0	2 ²¹ Network ID																					2 ⁸ Host ID												
Class D	1	1	1	0	2 ²⁸ Multicast Group ID																																
Class E	1	1	1	1	0	Reserved for Future Use																															

□ Eigenschaften

	Klasse A - Netz	Klasse B - Netz	Klasse C - Netz
Class ID (binär)	1 Bit = 0	2 Bit = 10	3 Bit = 110
Netz-ID (einschl. Class)	7 Bit (1 Byte)	14 Bit (2 Byte)	21 Bit (3 Byte)
Host ID	24 Bit (3 Byte)	16 Bit (2 Byte)	8 Bit (1 Byte)
Wertebereich (theoretisch)	0.0.0.0 bis 127.255.255.255	128.0.0.0 bis 191.255.255.255	192.0.0.0 bis 223.255.255.255
Anzahl Netze	126 (2 ⁷ -2)	16.382 (2 ¹⁴ -2)	2.097.150 (2 ²¹ -2)
Anzahl Rechner im Netz	16.777.214 (2 ²⁴ -2)	65.534 (2 ¹⁶ -2)	254 (2 ⁸ -2)

□ Internet Assigned Numbers Authority (IANA)

- Vergabe von IP-Adressen, Top-Level-Domains, IP-Protokollnummern, Portnummern
- Vergabe von IP-Adressbereichen an Regional Internet Registries (RIR)
[<http://www.iana.org/assignments/ipv4-address-space>]

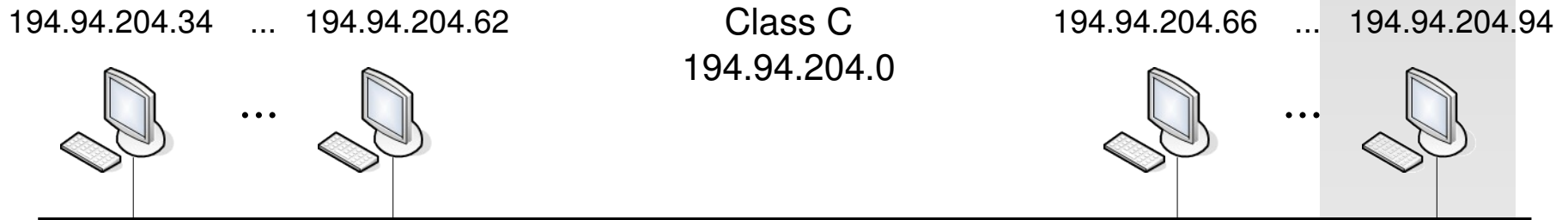
[IP-Adressbereiche]



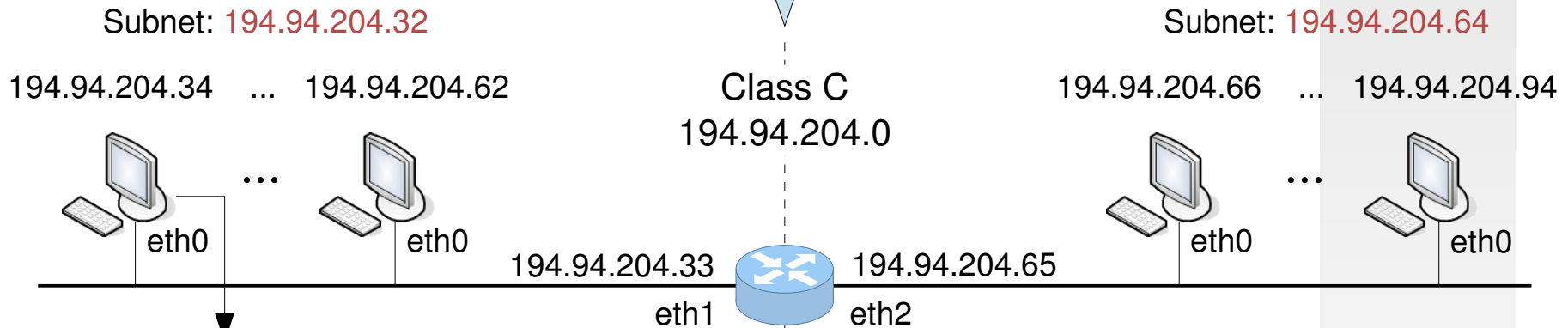
□ Regional Internet Registries (RIR)

- ARIN (American Registry for Internet Numbers)
- RIPE (Réseaux IP Européens Network Coordination Centre)
- APNIC (Asia Pacific Network Information Centre)
- LACNIC (Regional Latin-American and Caribbean IP Address Registry)
- AfriNIC (African Network Information Centre) für Afrika

Subnetting: Problemstellung



↓ Strukturierung

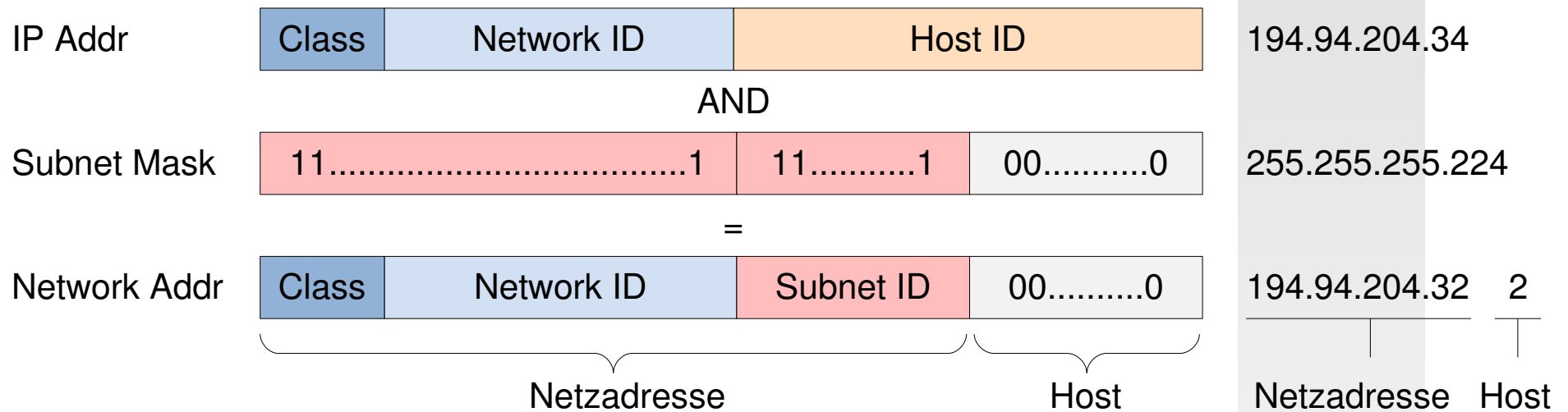


Destination	Next Hop	Interface
194.94.204.34	0.0.0.0	eth0
194.94.204.35	0.0.0.0	eth0
...
194.94.204.66	194.94.204.33	eth0
194.94.204.67	194.94.204.33	eth0
...

Destination	Next Hop	Interface
194.94.204.34	0.0.0.0	eth1
194.94.204.35	0.0.0.0	eth1
...
194.94.204.66	0.0.0.0	eth2
194.94.204.67	0.0.0.0	eth2
...

Subnetting: Subnet-Maske (1)

- Netze bestimmter Netzklasse mittels Subnet-Maske strukturierbar (RFC 950)



Beispiel

○ IP-Adresss	11000010 . 01011110 . 11001100 . 00100010	194. 94 .204. 34
○ Subnet-Maske	11111111 . 11111111 . 11111111 . <u>111</u> 00000	255.255.255. <u>224</u>
○ Netzadresse	11000010 . 01011110 . 11001100 . <u>001</u> 00000	194. 94 .204. <u>32</u>
○ Host ID	00000000 . 00000000 . 00000000 . 000 <u>00010</u>	<u>2</u>
○ Broadcast	11000010 . 01011110 . 11001100 . 00111111	194. 94 .204. <u>63</u>

Subnetting: Subnet-Maske (2)

□ allgemein

Subnet ID Bits	Host ID Bits	Subnetze	Subnet-Maske
1	7	2 (0)	128
2	6	4 (2)	192
3	5	8 (6)	224
4	4	16 (14)	240
5	3	32 (30)	248
6	2	64 (62)	252
7	1	128 (126)	254

← jeweiliges Octet
 - Class A: 2. Octet
 - Class B: 3. Octet
 - Class C: 4. Octet

im 4. Octet

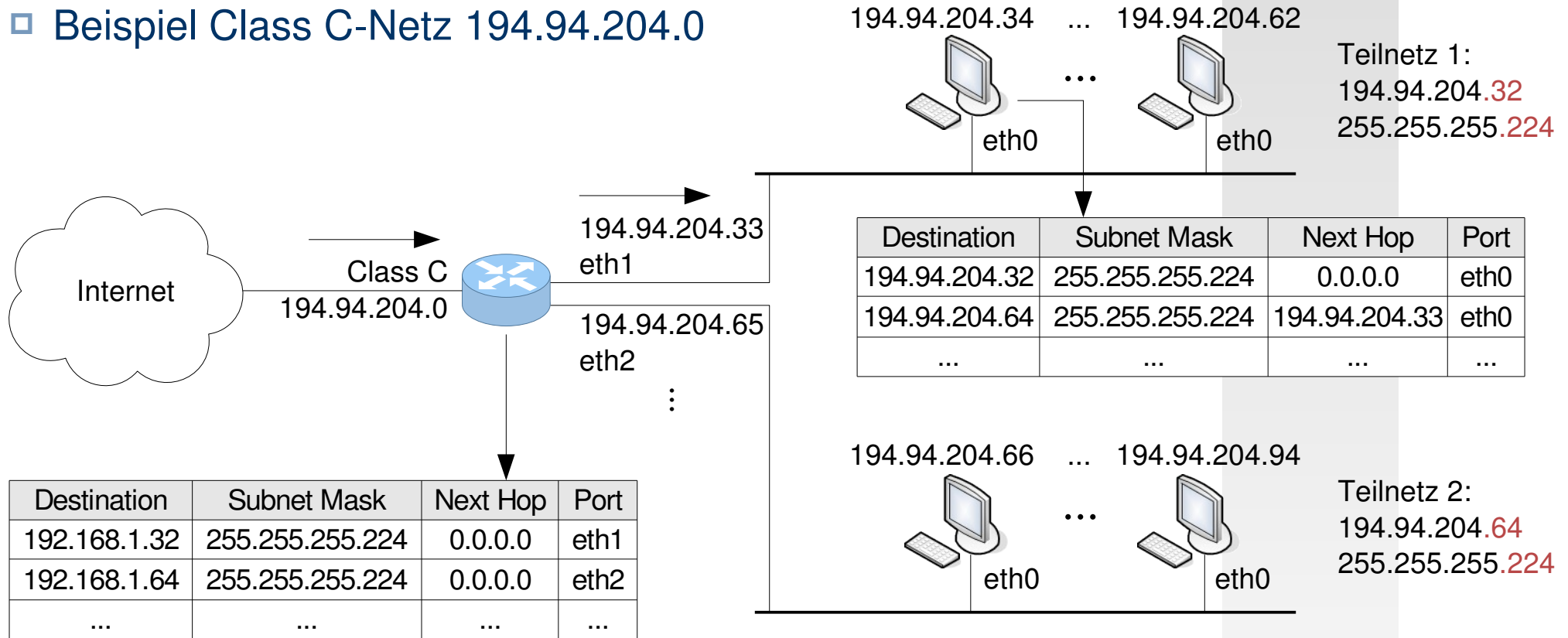
□ Beispiel Class C

Subnet ID Bits	Host ID Bits	Subnetze	Subnet-Maske	Host IDs
1	7	2 (0)	255.255.255.128	128 (126)
2	6	4 (2)	255.255.255.192	64 (62)
3	5	8 (6)	255.255.255.224	32 (30)
4	4	16 (14)	255.255.255.240	16 (14)
5	3	32 (30)	255.255.255.248	8 (6)
6	2	64 (62)	255.255.255.252	4 (2)
7	1	128 (126)	255.255.255.254	2 (0)

theoretische Zahl

tatsächlich nutzbare Zahl (RFC 950)

□ Beispiel Class C-Netz 194.94.204.0

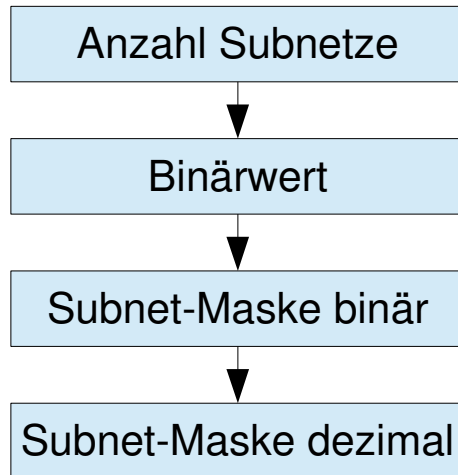


□ Routing im lokalen Netz

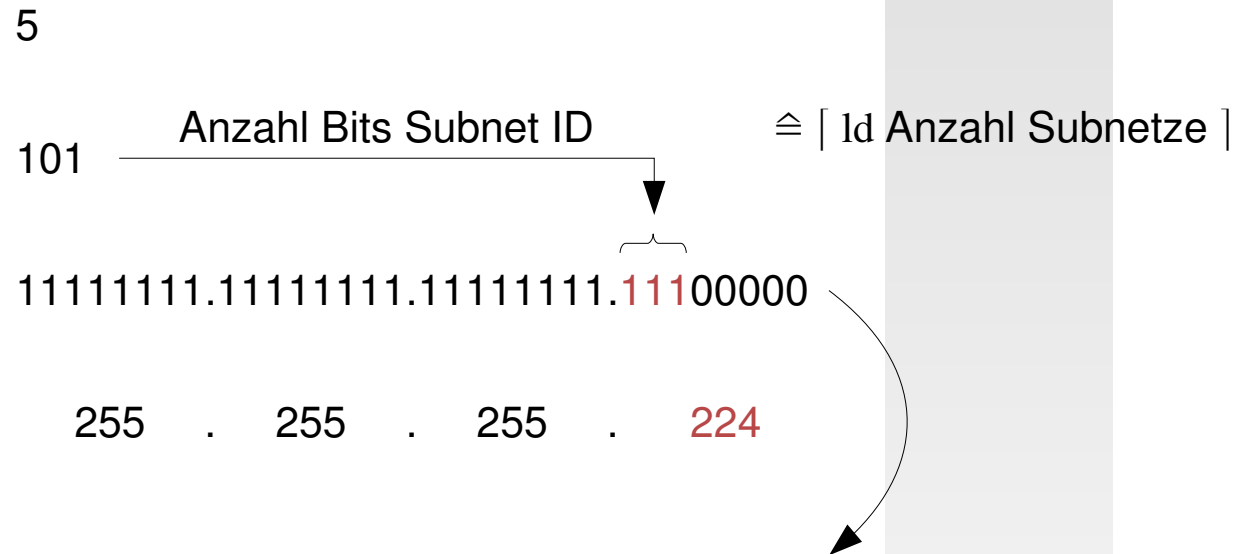
	Subnet Mask	Network Address	
Quelladresse	194.94.204.55	AND 255.255.255.224	= 194.94.204.32
1. Zieladresse	194.94.204.41	AND 255.255.255.224	= 194.94.204.32
2. Zieladresse	194.94.204.68	AND 255.255.255.224	= 194.94.204.64

direkt routen

□ Subnet-Maske ermitteln



Beispiel: 194.94.204.0



Subnet Mask 11111111.11111111.11111111.11100000 = 225.255.255.224

□ Network Adresses

- bei klassenbasierter Adressierung **ungültig** (RFC 950)
- bei klassenloser Adressierung nutzbar (RFC 1812)

11000010.01011110.11001100.~~00000000~~ = ~~194.94.204.0~~

~~.00100000~~ = ~~194.94.204.32~~

~~.01000000~~ = ~~194.94.204.64~~

~~.01100000~~ = ~~194.94.204.96~~

~~.10000000~~ = ~~194.94.204.128~~

~~.10100000~~ = ~~194.94.204.160~~

~~.11000000~~ = ~~194.94.204.192~~

~~.11100000~~ = ~~194.94.204.224~~

- klassenbasierte Adressierung unflexibel:
 - begrenzte Anzahl Netze je Klasse und feste Anzahl Adressen je Netz
 - Strukturierung innerhalb des Adressbereiches einer Klasse nicht möglich
 - anwachsende Routing-Tabellen aufgrund fehlender Routenaggregation
 - feste Größe von NetworkID und HostID entsprechend Klasse

- verschiedene Adressbereiche reserviert, z.B:

Bedeutung	Adressen	Bemerkung
Private Use	10.0.0.0 ... 10.255.255.255	1 Class A-Netz
Public Data	14.0.0.0 ... 14.255.255.255	1 Class A-Netz
Cable TV	24.0.0.0 ... 24.255.255.255	1 Class A-Netz
Loopback	127.0.0.0 ... 127.255.255.255	1 Class A-Netz
Link Local	169.254.0.0 ... 169.254.255.255	1 Class B-Netz
Private Use	172.16.0.0 ... 172.31.255.255	16 Class B-Netze
Private Use	192.168.0.0 ... 192.168.255.255	256 Class C-Netze
...
Multicast	224.0.0.0 ... 239.255.255.255	

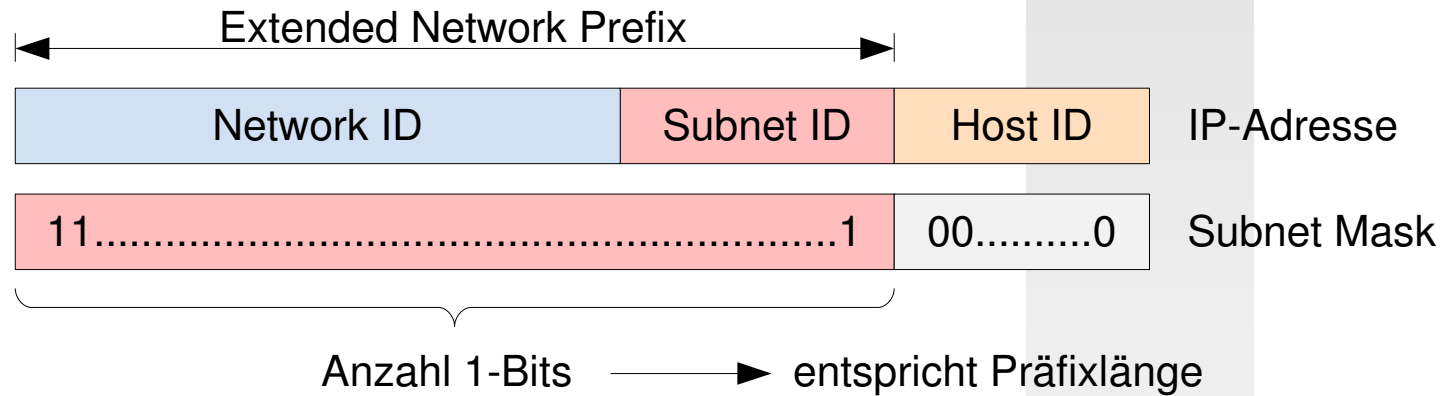
[<http://tools.ietf.org/html/rfc3330>]

□ Netzwerkpräfix

- ohne Subnetting



- mit Subnetting



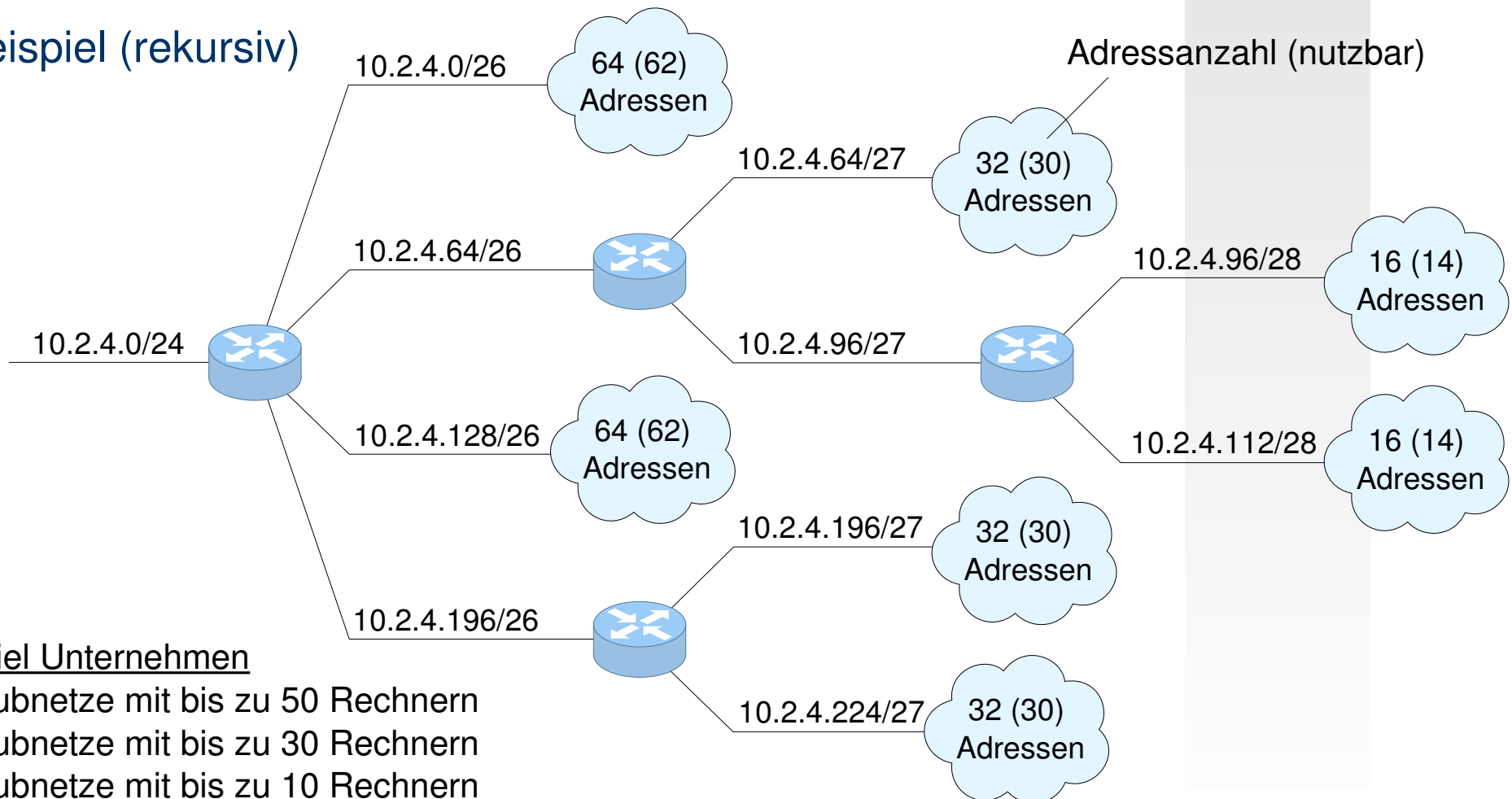
□ Netzwerkpräfixnotation:

<Network Address>/<Prefix Length>

- 192.168.2.0/24 24 Bit Network ID, 8 Bit Host ID (entspricht Class C)
- 192.168.2.0/26 26 Bit Network ID, 6 Bit Host ID (entspricht Class C Subnetting)
- 192.168.2.0/23 23 Bit Network ID, 9 Bit Host ID (entspricht Class C Supernetting)

- VLSM - Variable Length Subnet Mask (RFC 1009)
 - erlaubt Subnet-Masken verschiedener Länge in privaten IP-Netzen
 - ermöglicht hierarchische Zerlegung eines zugewiesenen Adressbereiches

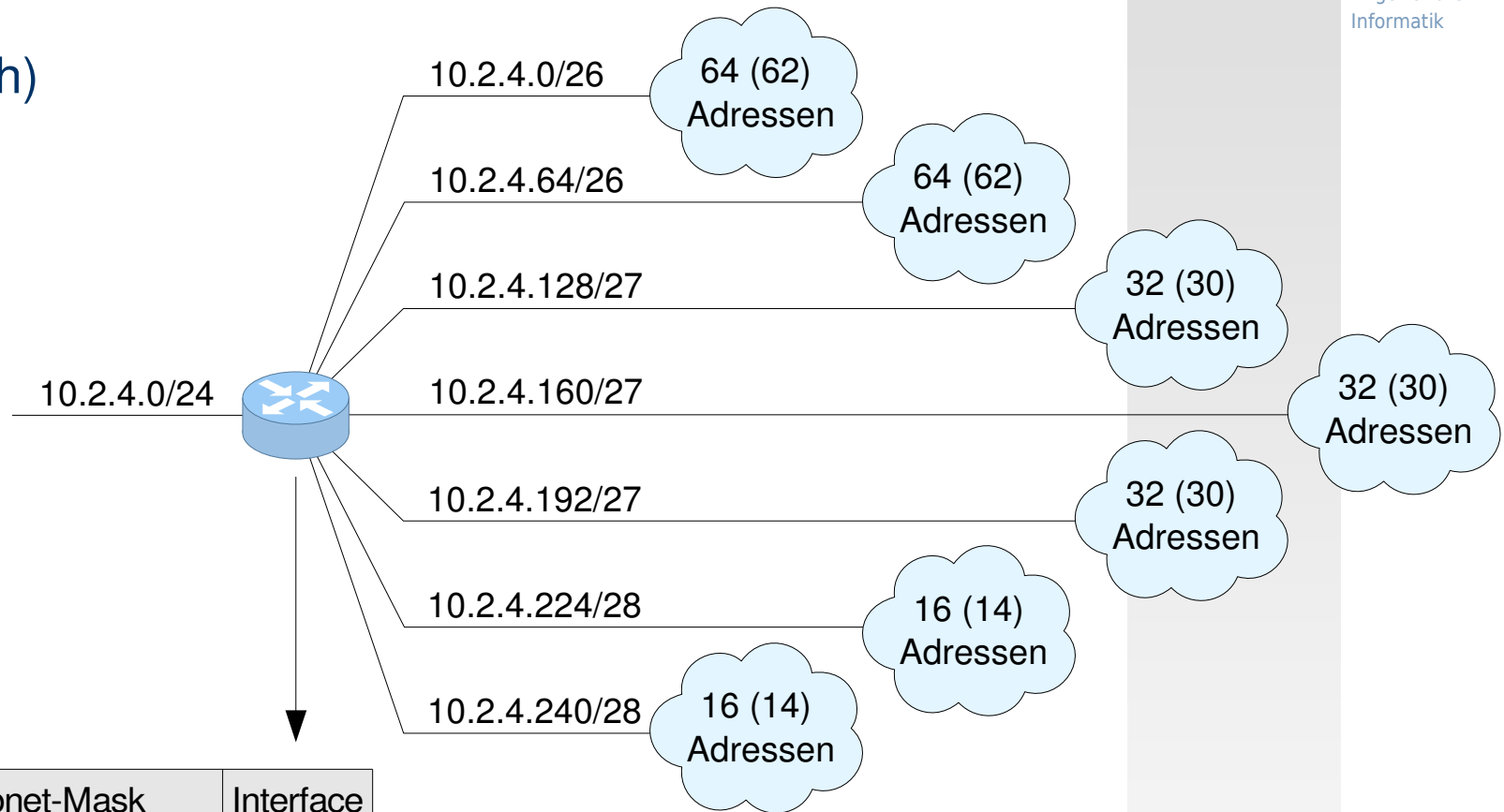
□ Beispiel (rekursiv)



Beispiel Unternehmen

- 2 Subnetze mit bis zu 50 Rechnern
- 3 Subnetze mit bis zu 30 Rechnern
- 2 Subnetze mit bis zu 10 Rechnern

□ Beispiel (flach)



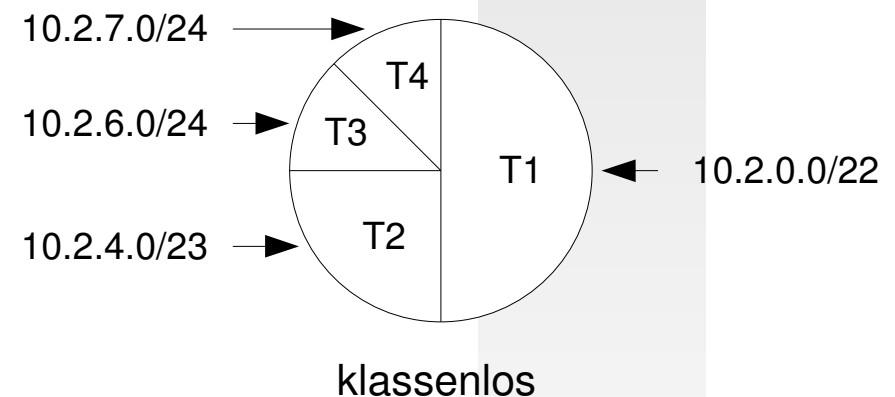
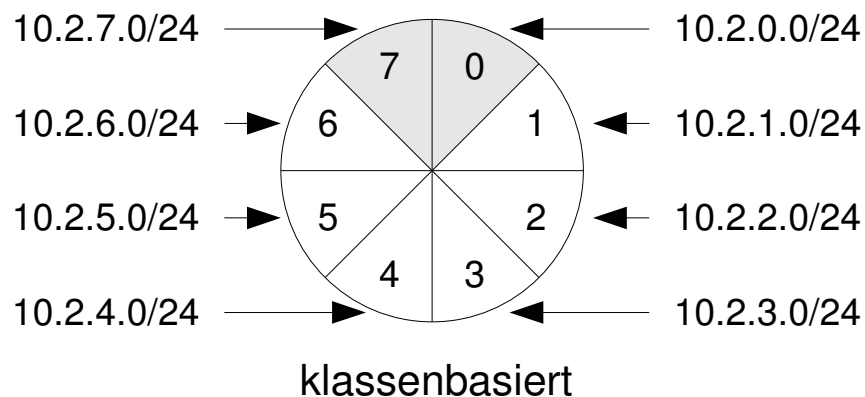
Destination	Subnet-Mask	Interface
10.2.4.0/26	255.255.255.192	1
10.2.4.64/26	255.255.255.192	2
10.2.4.128/27	255.255.255.224	3
10.2.4.160/27	255.255.255.224	4
10.2.4.192/27	255.255.255.224	5
10.2.4.224/28	255.255.255.240	6
10.2.4.240/28	255.255.255.240	7

Beispiel Unternehmen

- 2 Subnetze mit bis zu 50 Rechnern
- 3 Subnetze mit bis zu 30 Rechnern
- 2 Subnetze mit bis zu 10 Rechnern

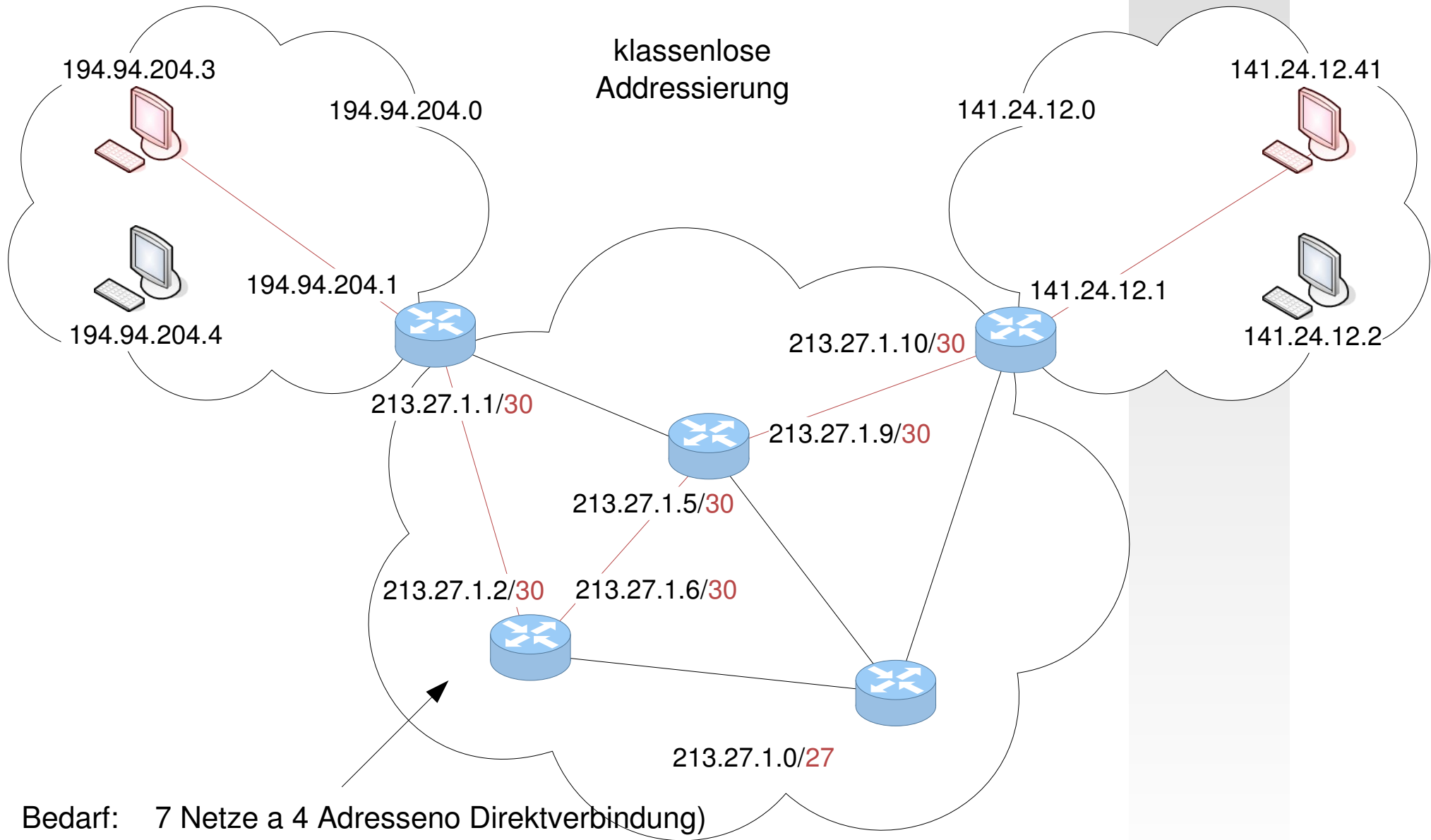
- Classless Interdomain Routing – CIDR (RFC 1517-1520)
 - Nutzung VLSM in öffentlichen IP-Netzen mittels Netzwerkpräfixnotation
 - beliebige Zerlegung eines gegebenen Adressbereiches **entsprechend Netztopologie**

□ Beispiel: 10.2.0.0/21



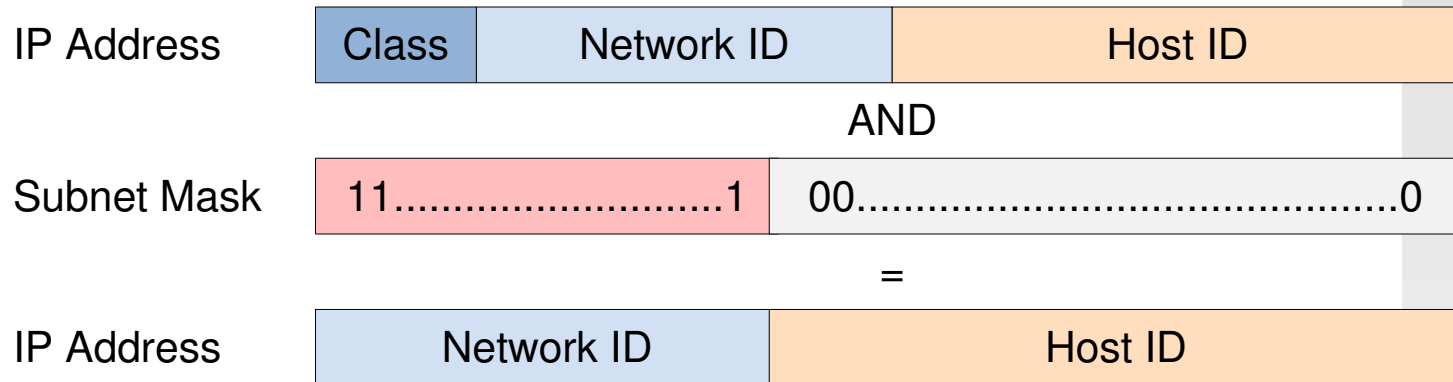
□ Anforderungen

- Routing-Protokolle müssen CIDR unterstützen
- Weiterleitung in Routern muss Longest Prefix Match unterstützen
- Adresszuweisungen müssen zur Routenaggregation Netztopologie berücksichtigen

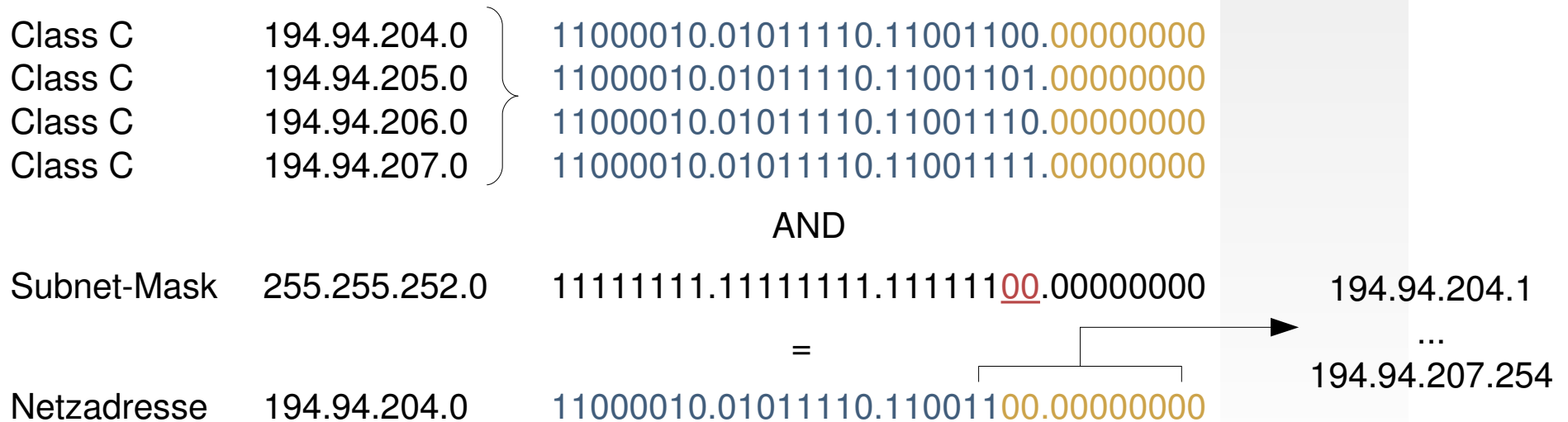


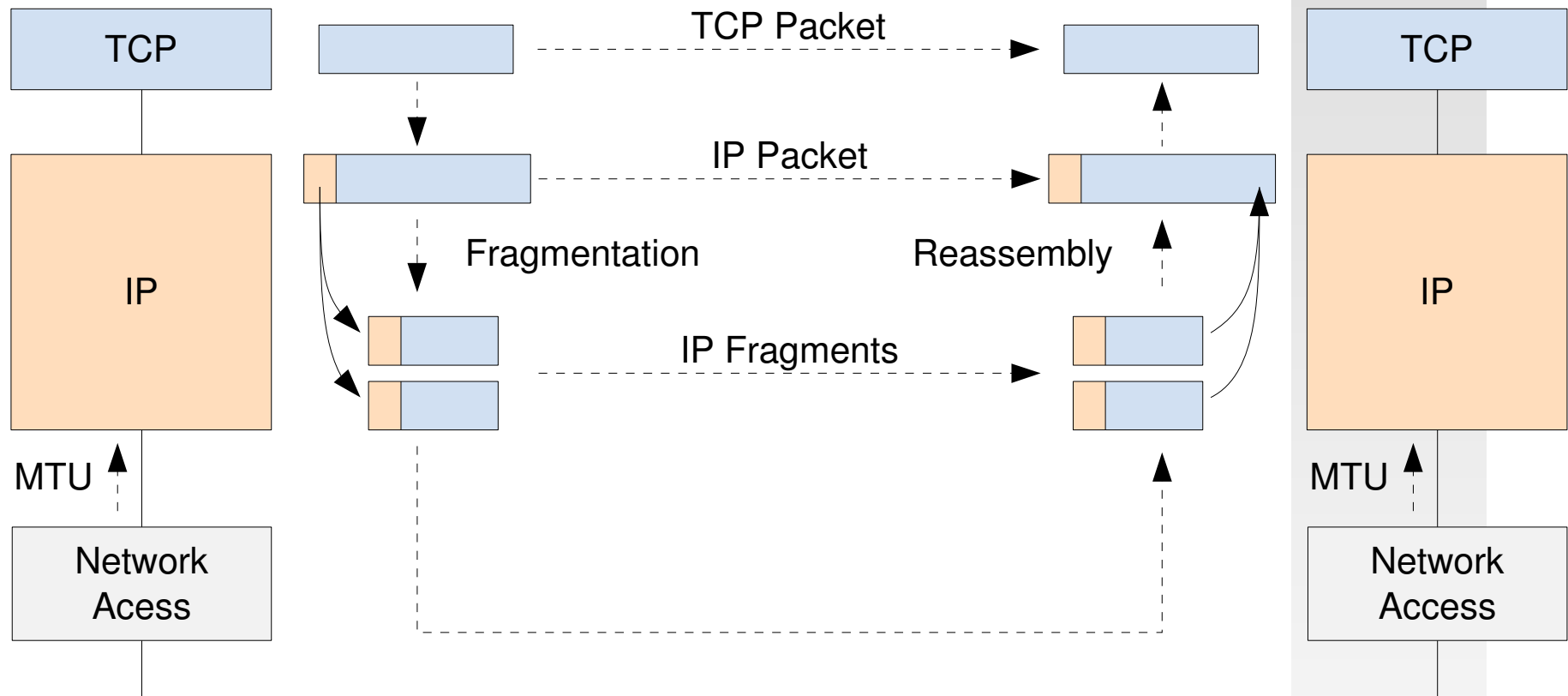
Bedarf: 7 Netze a 4 Adressen (Direktverbindung)
28 Adressen

□ Zusammenfassen linearer IP-Adressbereiche



□ Beispiel





□ nicht transparente Fragmentierung

- kein Zusammensetzen in Zwischensystemen
- erneute Fragmentierung, wenn fragmentiertes Paket zu groß
- damit nicht transparent für nachfolgende Übertragungsabschnitte

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version		IHL		Type of Service				Total Length																							
Identification								Flags		Fragment Offset																					
Time to Live				Protocol				Header Checksum																							
Source Address																															
Destination Address																															
Option												Padding																			
IP Payload (z.B. TCP)																															

□ Identification

- Nummerierung des IP-Paketes
- eindeutig für gegebenes Quell-/Zieladresspaar

□ Fragment Offset

- Position Daten innerhalb Nutzlast des IP-Paketes
- gemessen in 8 Byte-Blöcken

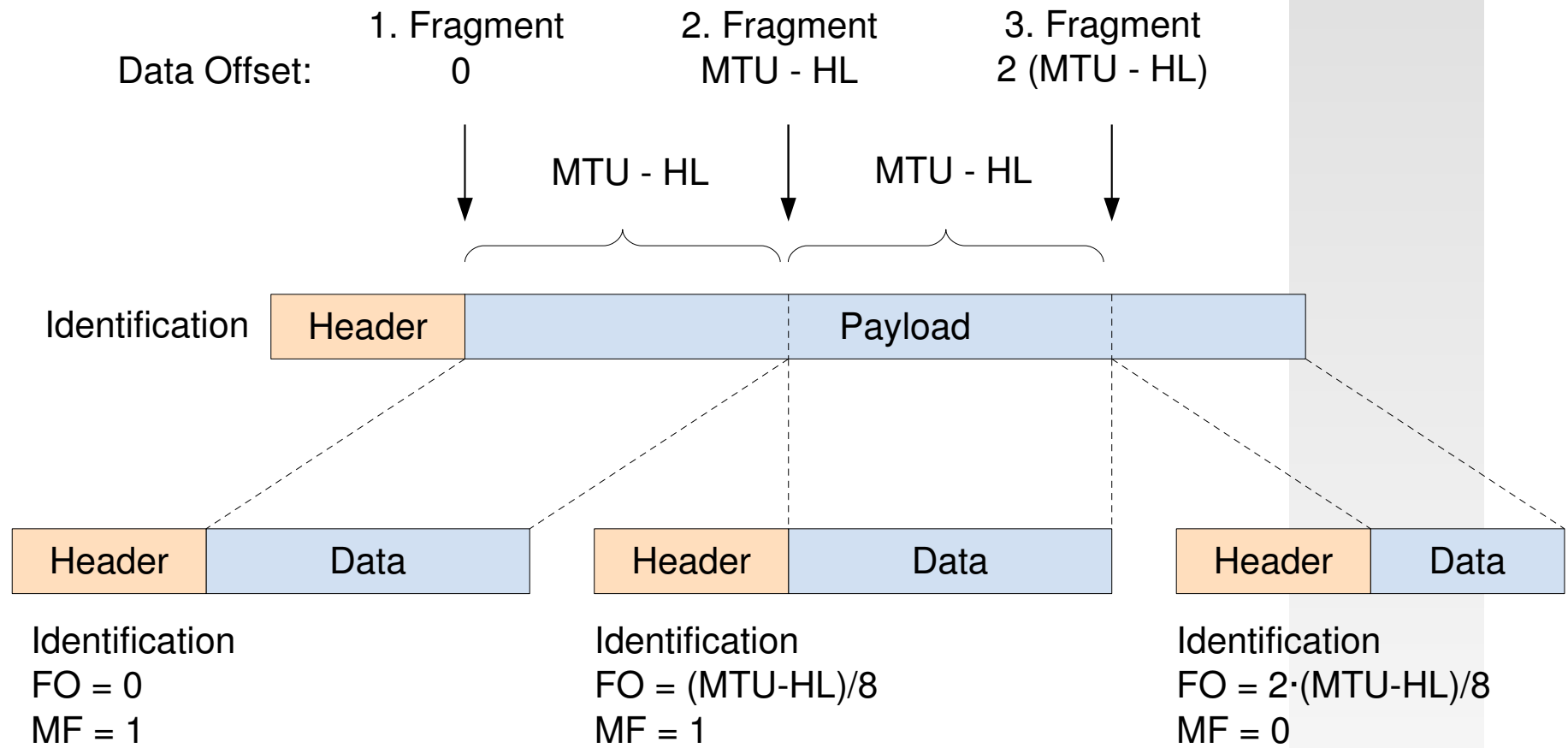
□ Flags



Flags

- 0: Last Fragment
- 1: More Fragments
- 0: May Fragment
- 1: Don't Fragment

Fragmentierung: Informationen im IP-Header (2)

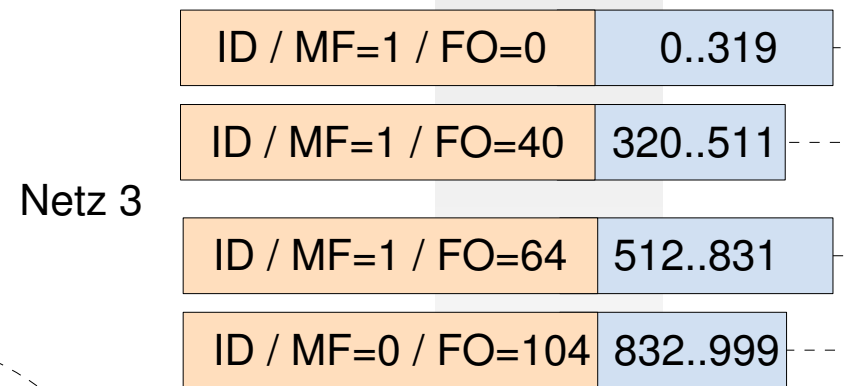
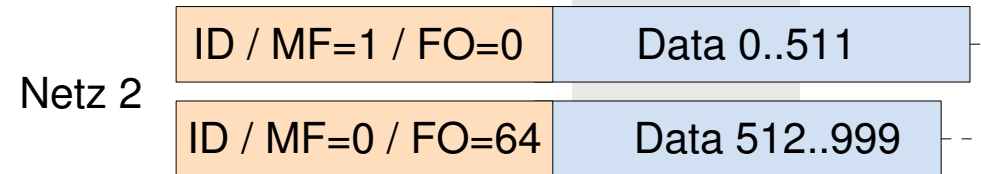
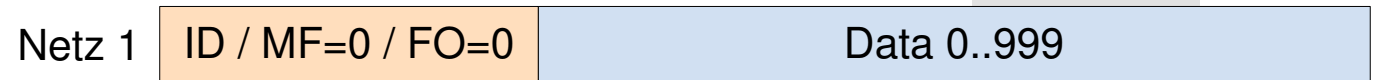


MTU

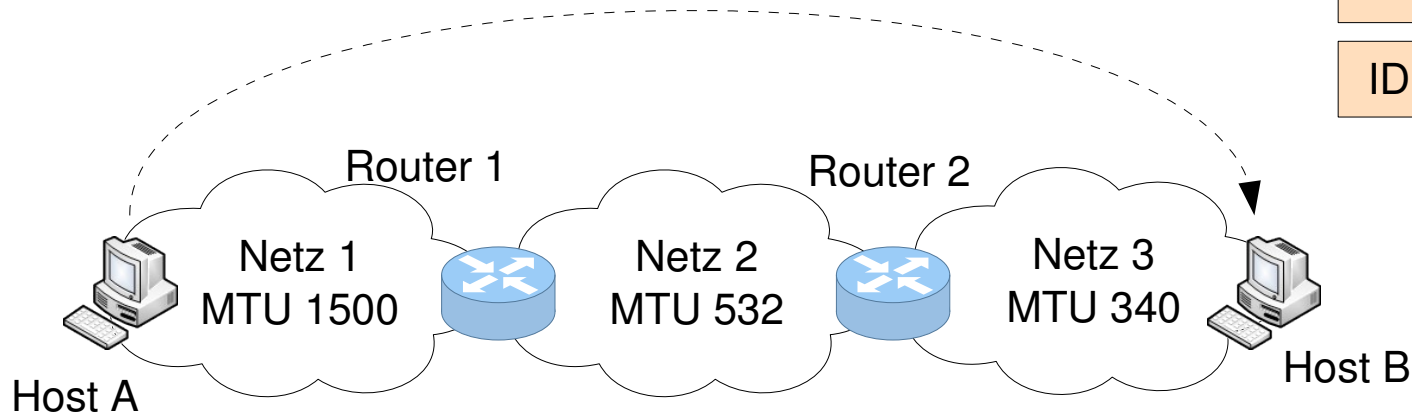
FO – Fragment Offset
HL – Header Length = 4 IHL
MF – More Fragments Flag
MTU – Maximum Transmission Unit

□ Paket

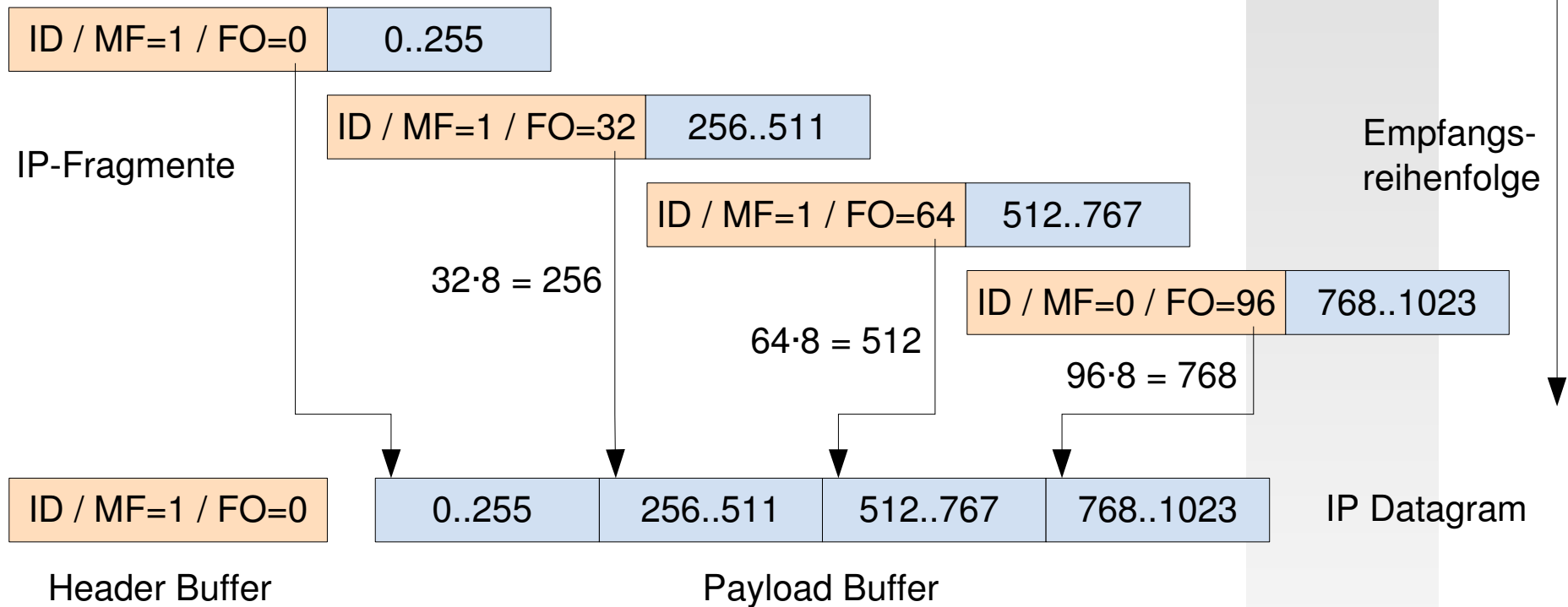
- Länge: 1020 Byte
- Header: 20 Byte
- Nutzlast: 1000 Byte



□ Übertragungsstrecke

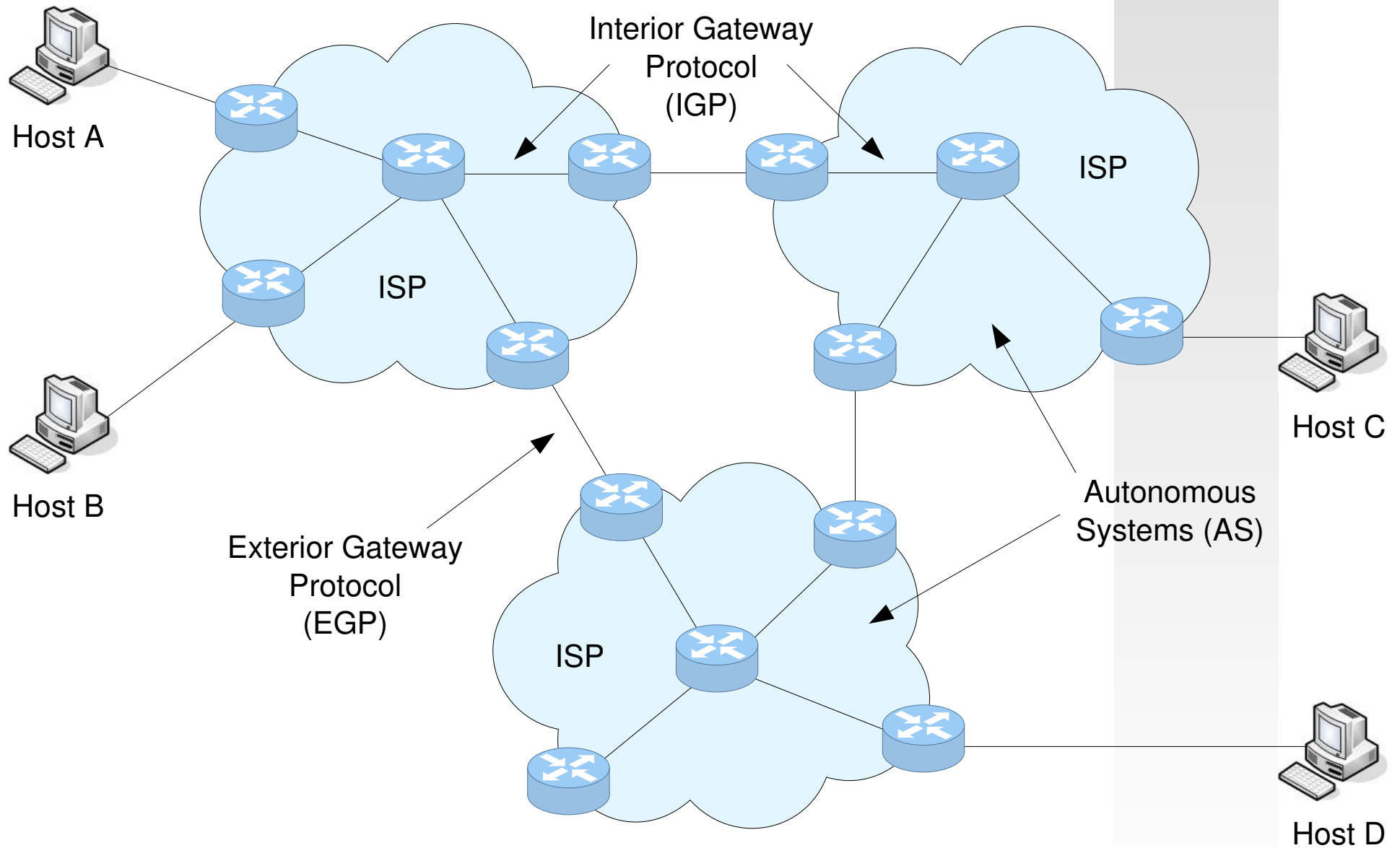


□ Prinzip



□ Probleme

- ungesicherte Reihenfolge der Fragmente
- Reservierung von Ressourcen, Freigabe erst nach Timeout



□ statisches Routing

- Routing-Tabellen manuell konfiguriert
- kein Re-Routing im Fehlerfall

□ dynamisches Routing

- Anpassung an aktuelle Netzsituation und Re-Routing im Fehlerfall
- Nachbarknoten tauschen Topologie-Informationen mittels Routing-Protokollen aus

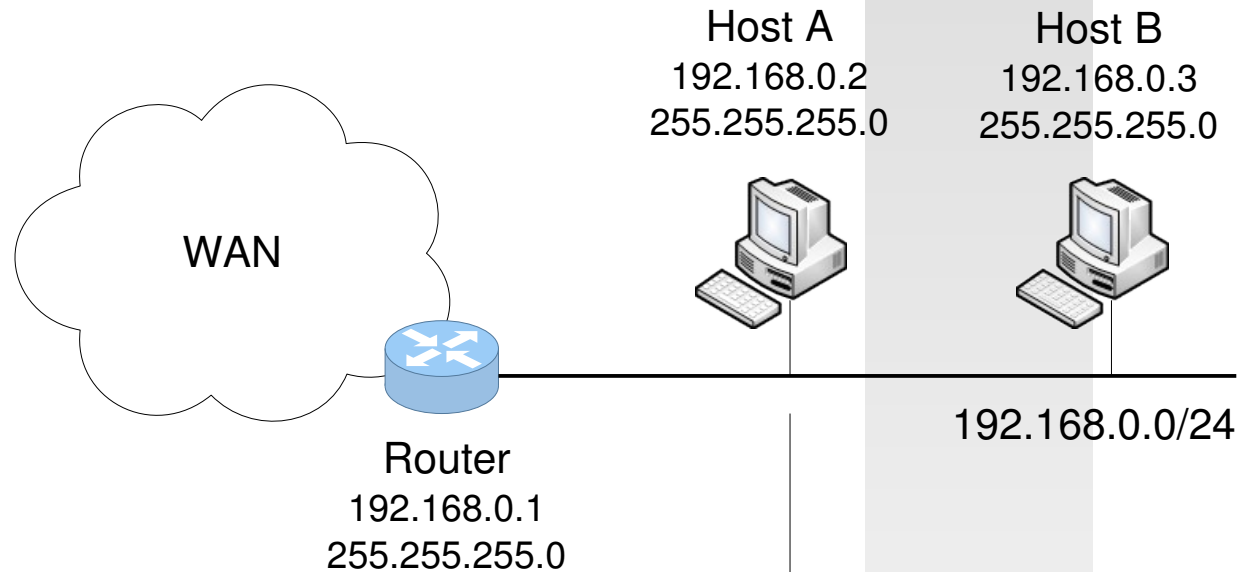
Routing-Protokoll	Routing-Vefahren	Routing-Algorithmus	Einsatz	Metrik	Anmerkungen
BGP	Path Vector	Bellman-Ford	EGP	Policies	de Facto-Standard
RIP	Distance Vector	Bellman-Ford	IGP	Hop-Count	Count-to-Infinity-Problem
OSPF	Link State	Dijkstra	IGP	*	hierarchisches Routing
IS-IS	Link State	Dijkstra	IGP	*	ISO-Standard, vglb. mit OSPF

* verschiedene kombinierbare Metriken

BGP - Border Gateway Protocol
RIP - Routing Information Protocol
OSPF - Open Shortest Path First

□ Informationen je Eintrag

- Zielnetz
- Netzmaske
- nächster Router
- Netzwerk-Interface
- Metrik



□ Beispiel Host A

Destination	Netmask	Next Hop	Interface	Metrik
192.168.0.0	255.255.255.0	0.0.0.0	eth0	0
127.0.0.0	255.0.0.0	0.0.0.0	lo	0
0.0.0.0	0.0.0.0	192.168.0.1	eth0	0

← Eigenes Netz

Loopback Device (eigener Rechner)

Default Route

□ Definition: **Metrik**

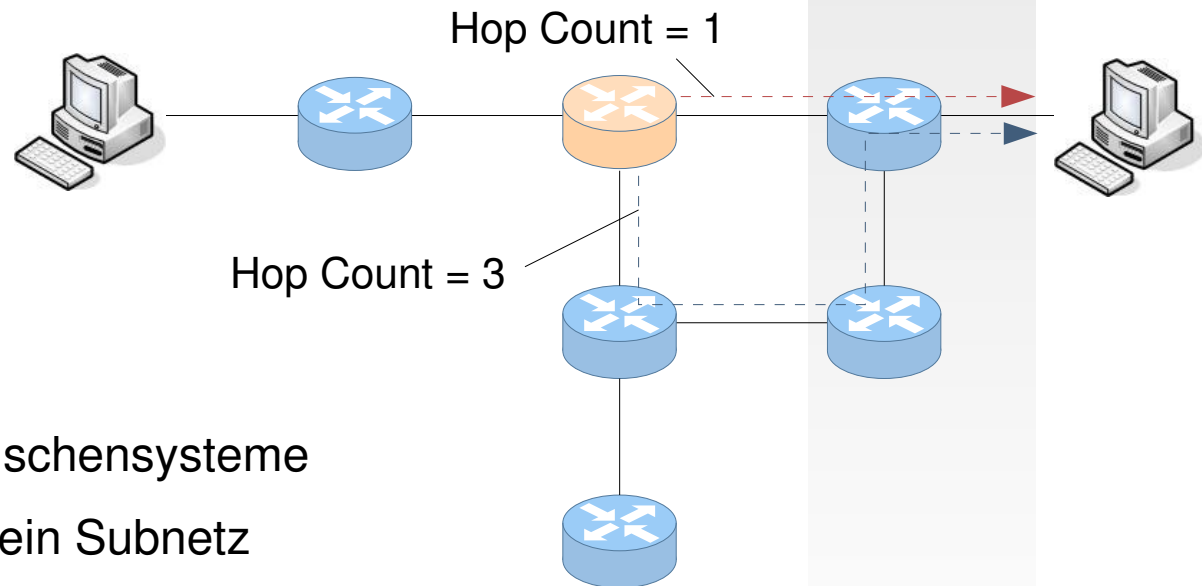
- definiert das Maß für die Bewertung einer Verbindung
- dient Routing-Algorithmus zur Ermittlung der besten Route

□ verschiedene Informationen als Metrik nutzbar (auch Kombinationen)

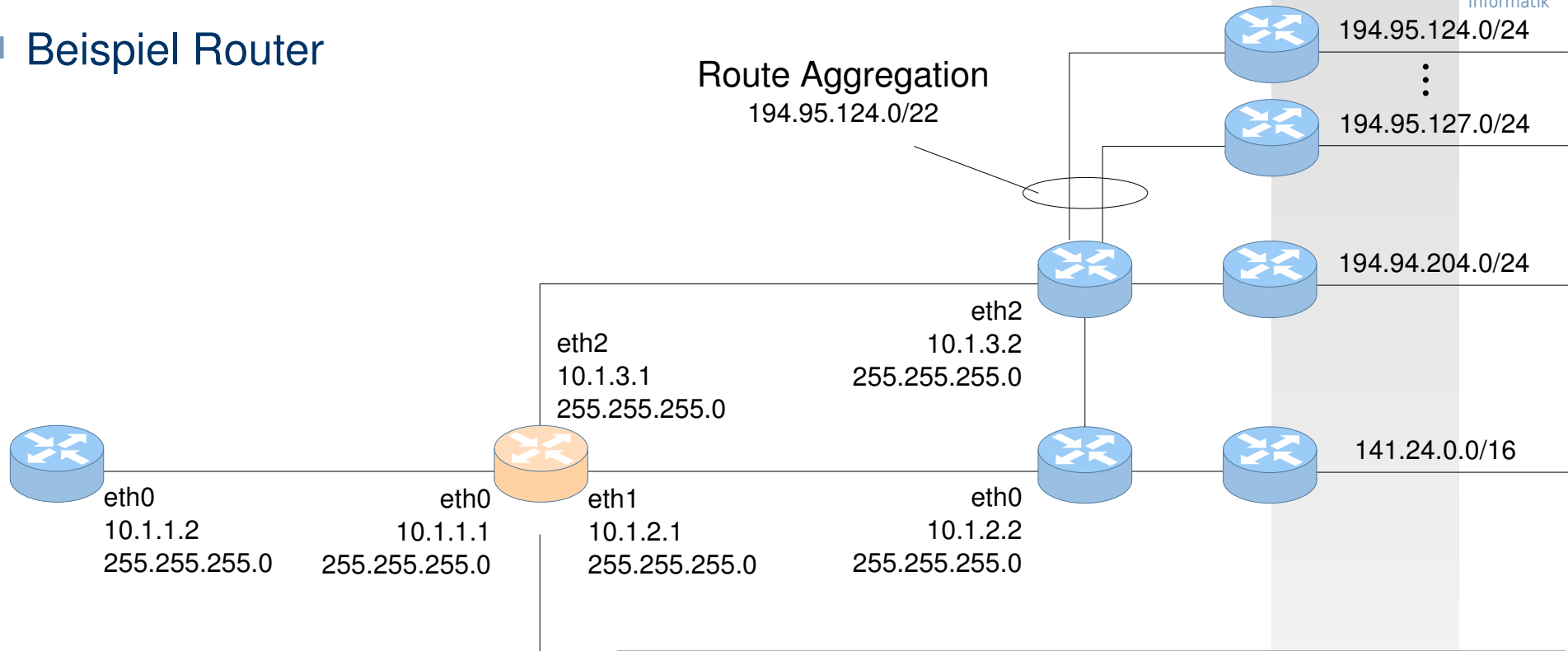
- Hop-Count
- Bandbreite
- Verzögerung
- Zuverlässigkeit
- Kosten

□ Hop-Count:

- Anzahl zu durchlaufender Zwischensysteme
- alternativ: Anzahl Sprünge in ein Subnetz



□ Beispiel Router

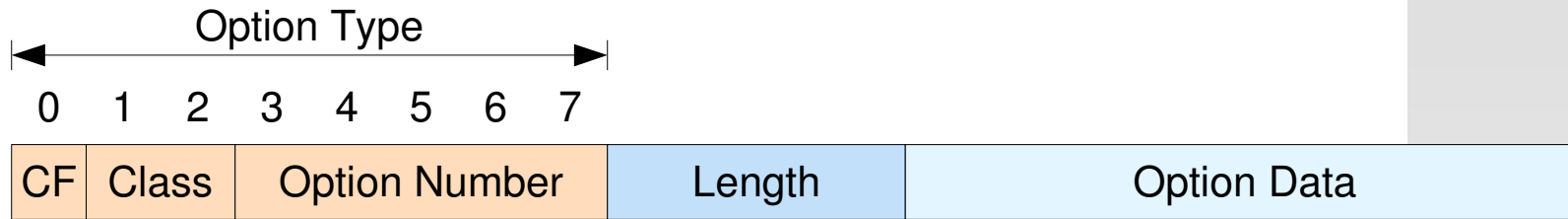


Destination	Netmask	Next Hop	Interface	Metrik
141.24.0.0/16	255.255.0.0	10.1.2.2	eth1	2
141.24.0.0/16	255.255.0.0	10.1.3.2	eth2	3
194.94.204.0/24	255.255.255.0	10.1.3.2	eth2	2
194.94.204.0/24	255.255.255.0	10.1.2.2	eth1	3
194.95.124.0/22	255.255.252.0	10.1.3.2	eth2	2
0.0.0.0	0.0.0.0	10.1.1.2	eth0	0

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version				IHL			Type of Service					Total Length																			
Identification												Flags			Fragment Offset																
Time to Live						Protocol						Header Checksum																			
Source Address																															
Destination Address																															
Options																							Padding								
IP Payload (z.B. TCP)																															

□ Optionen

- spezielle Informationen
- variable Länge
- max. 40 Byte

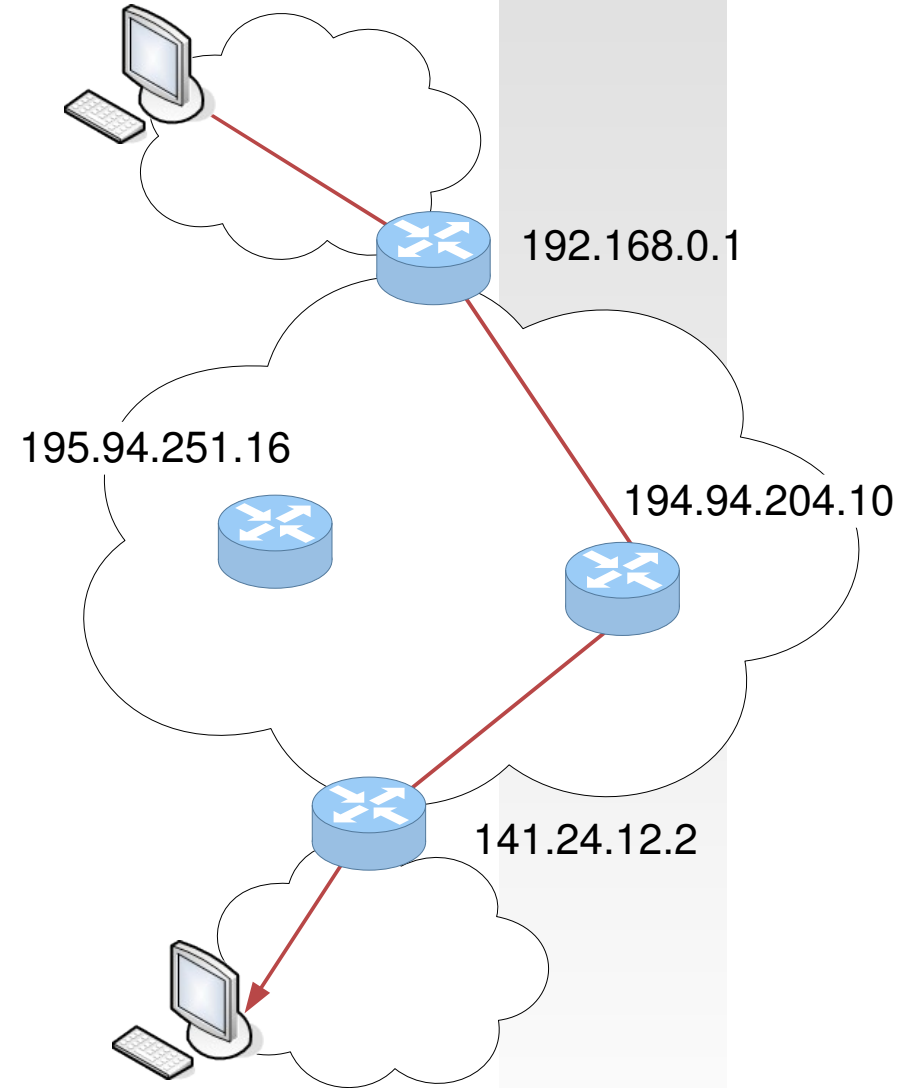
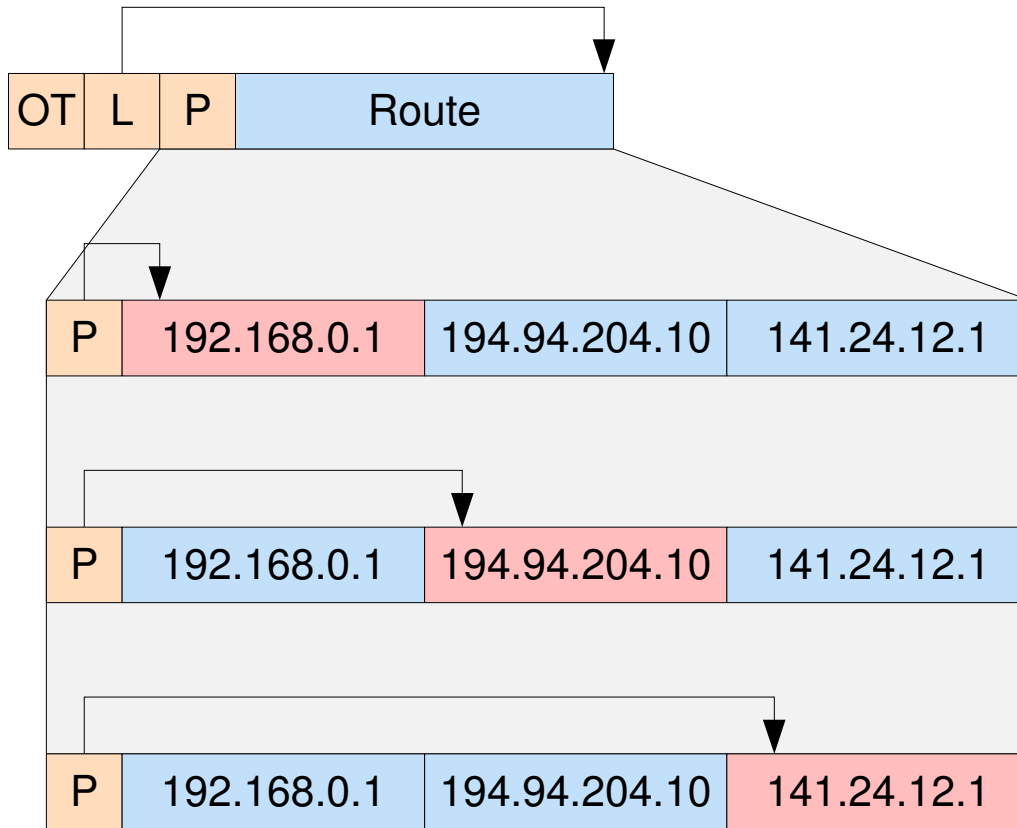


Class	Number	Length	Description
0	0	-	End of Option List
0	1	-	No Operation.
0	2	11	Security
0	3	variabel	Loose Source Routing
0	7	variabel	Record Route
0	8	4	Stream ID
0	9	variabel	Strict Source Routing
2	4	variabel	Internet Timestamp

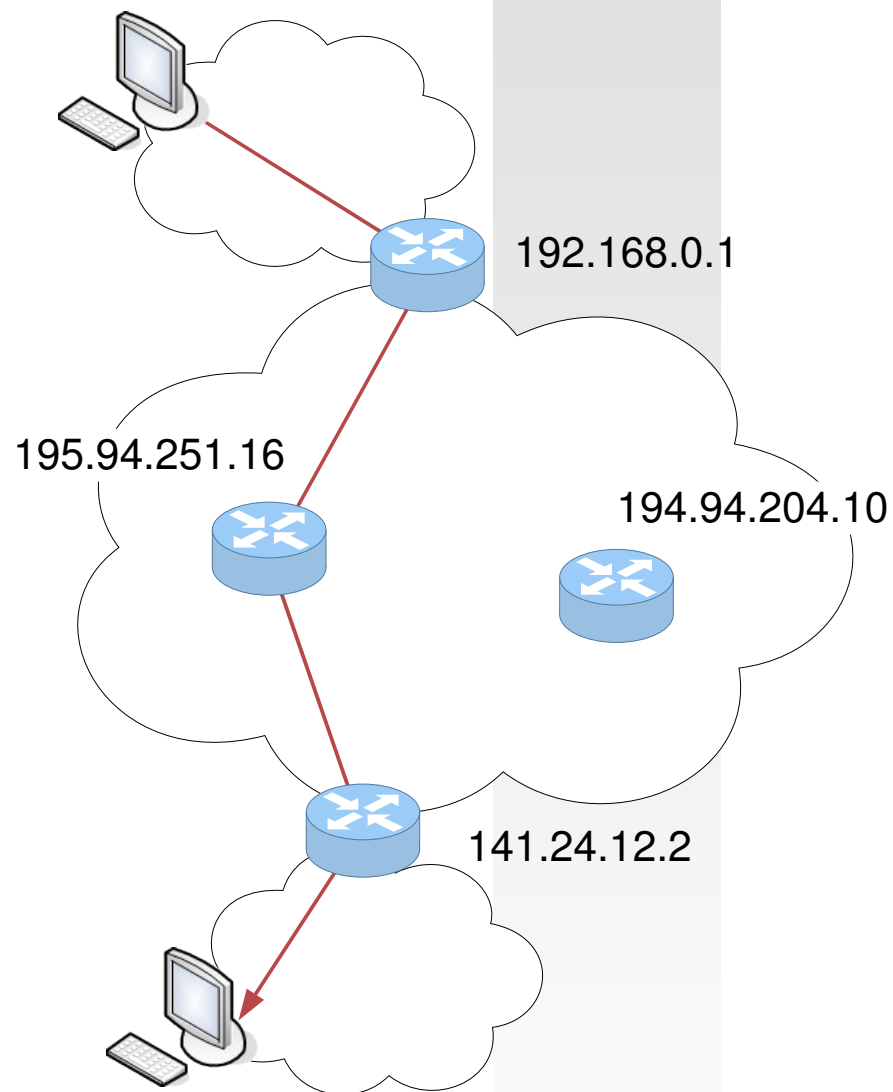
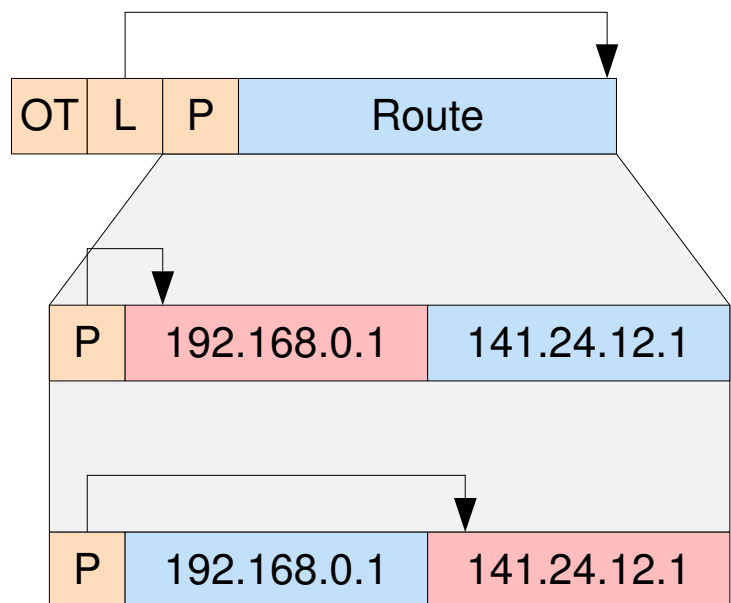
0 – Control
 1 – Reserved
 2 – Debugging and Measurement
 3 – Reserved

Copied Flag 0 – Kopie nur im 1. Fragment
 1 – Kopie in allen Fragmenten

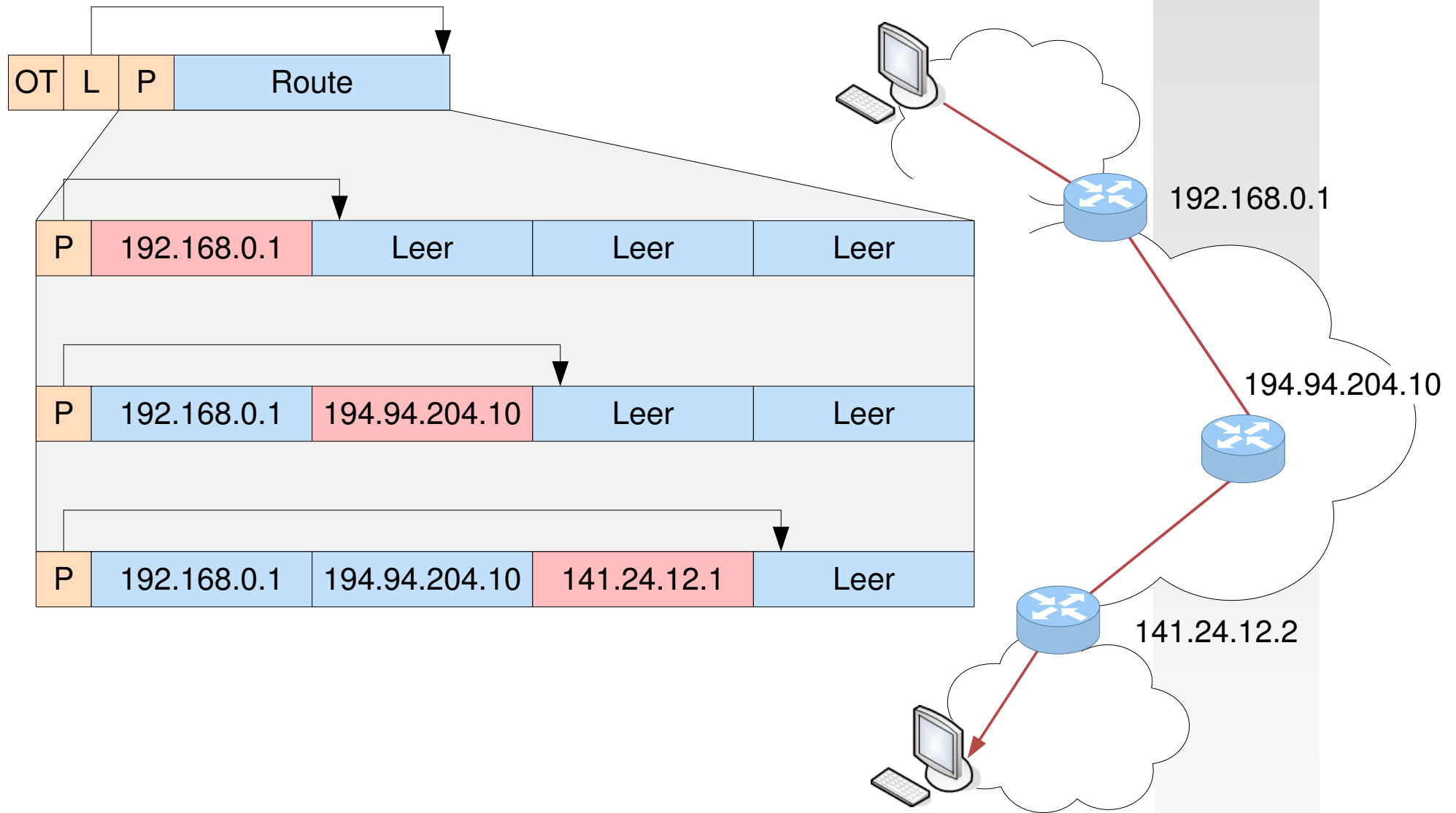
IPv4-Header Optionen: Strict Source Routing



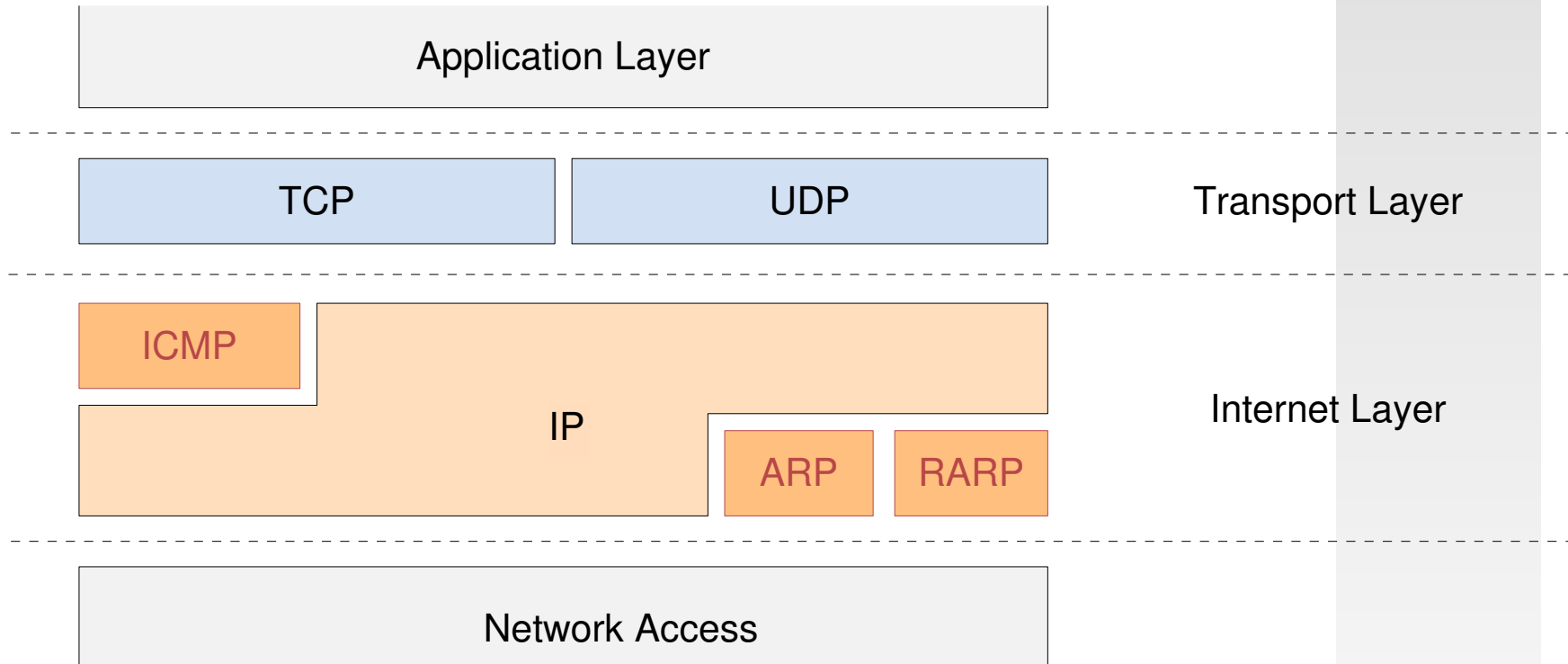
IPv4-Header Optionen: Loose Source Routing



IPv4-Header Optionen: Recording Route



□ Protokollstack



IP - Internet Protocol
TCP - Transport Control Protocol
UDP - User Datagram Protocol

ICMP - Internet Control Message Protocol
ARP - Address Resolution Protocol
RARP - Reverse Address Resolution Protocol

□ Implementierungsvorgaben: RFC 1122

IP ist nicht alleine

□ Aufgaben

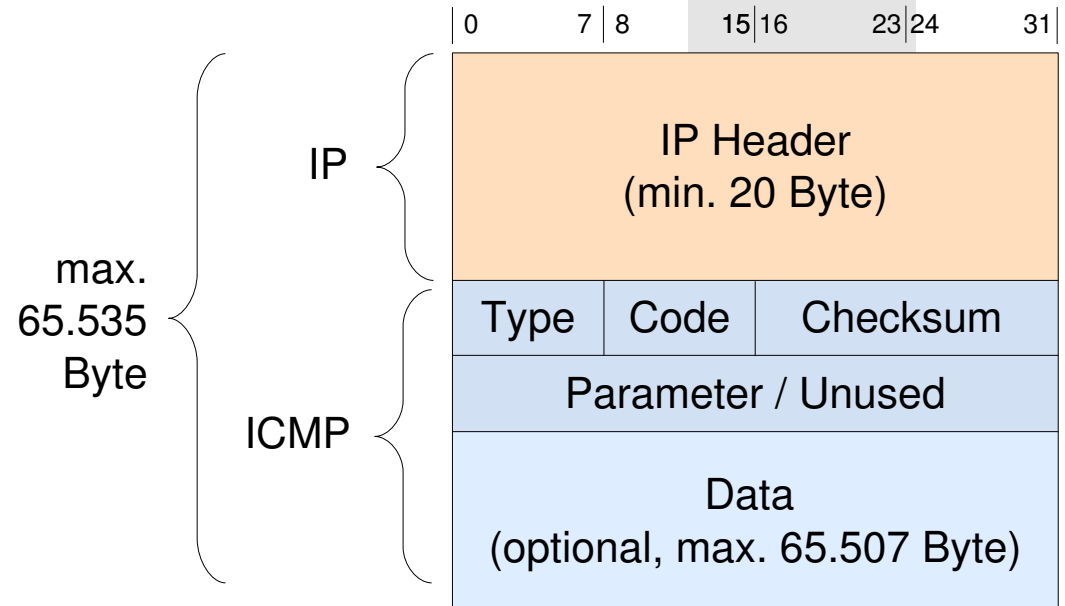
- Fehler- und Informationsmeldungen
- Unterstützung Diagnose
- Aufzeichnung von Zeitmarken
- Verwaltung Routing-Tabellen
- Berichtigung Flusskontrolle

□ Standard: RFC 792 (1981)

□ Format

- Type: Typ der ICMP-Nachricht
- Code: nähere Erläuterung (wenn nicht genutzt = 0)
- Checksum: über komplette ICMP-Nachricht (zur Berechnung = 0)
- Daten: abhängig von Type

ICMP als Nutzlast von IP

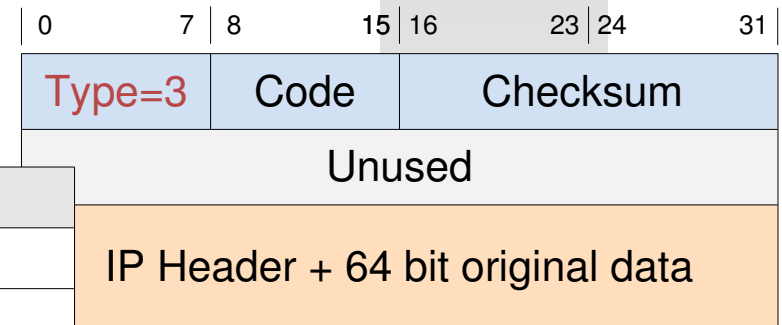


Type	Name	Type	Name
0	Echo Reply	19	Reserved (for Security)
3	Destination Unreachable	20-29	Reserved (for Robustness Experiment)
4	Source Quench	30	Traceroute
5	Redirect	31	Datagram Conversion Error
6	Alternate Host Address	32	Mobile Host Redirect
8	Echo	33	IPv6 Where-Are-You
9	Router Advertisement	34	IPv6 I-Am-Here
10	Router Solicitation	35	Mobile Registration Request
11	Time Exceeded	36	Mobile Registration Reply
12	Parameter Problem	37	Domain Name Request
13	Timestamp	38	Domain Name Reply
14	Timestamp Reply	39	SKIP
15	Information Request	40	Photuris
16	Information Reply	41	ICMP messages utilized by experimental
17	Address Mask Request	42-255	Reserved
18	Address Mask Reply		

[<http://www.iana.org/assignments/icmp-parameters>]

Destination Unreachable (Type=3)

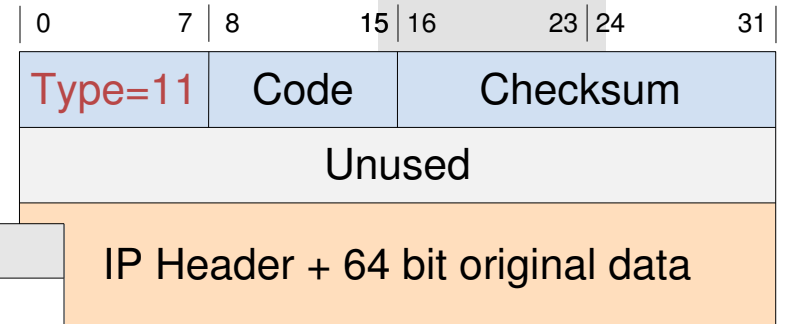
Code	Meaning
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network Prohibited
10	Communication with Destination Host Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service
13	Communication Administratively Prohibited
14	Host Precedence Violation
15	Precedence cutoff in effect



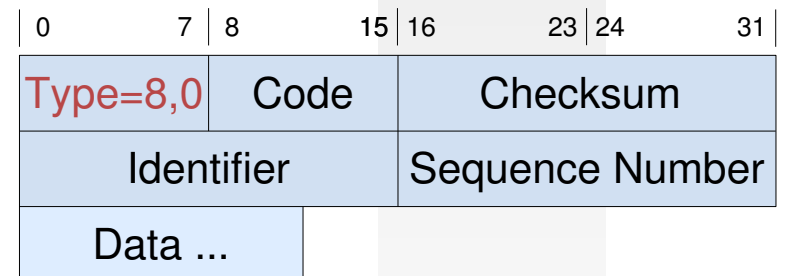
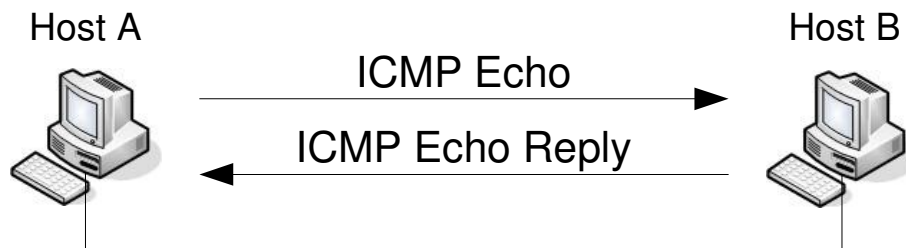
Time Exceeded (Type=11)

- TTL in IP-Header wird in Zwischensystem 0
- bei Verlust IP-Fragment Timeout im Empfänger

Code	Meaning
0	Time To Live exceeded in transmit
1	Fragment reassembly time exceeded



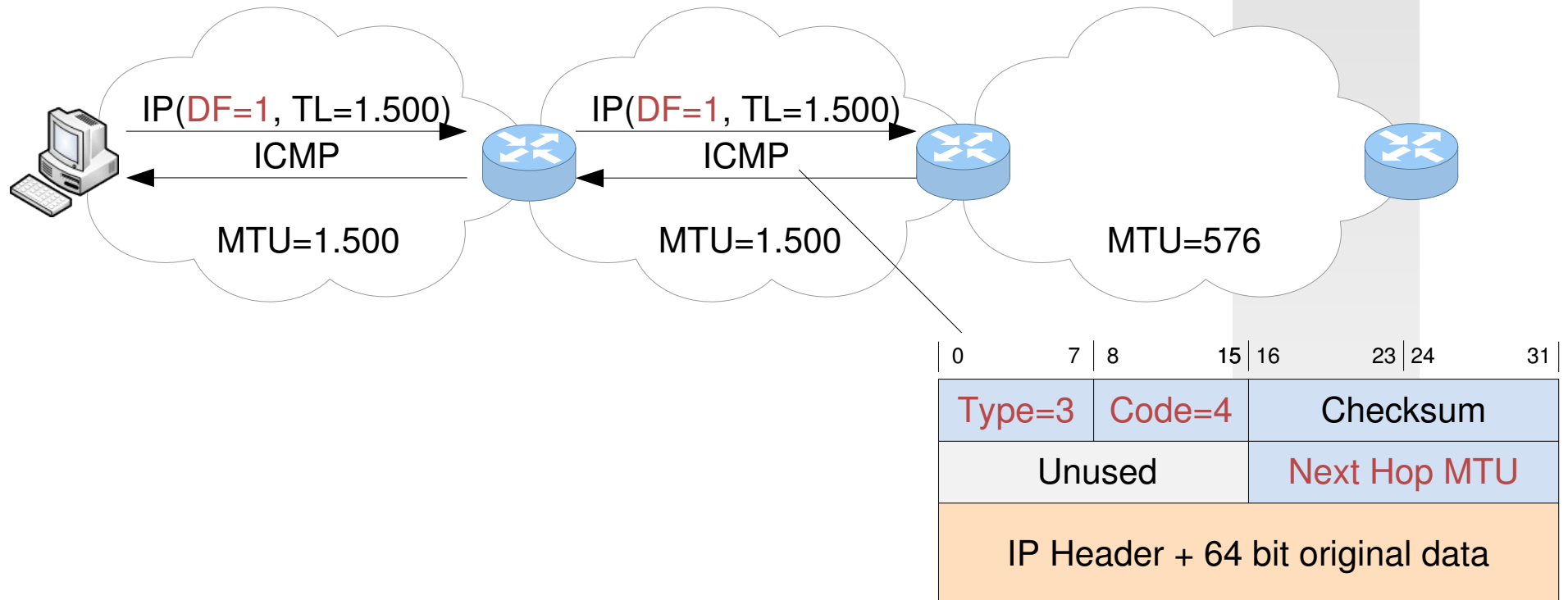
Echo Request / Echo Reply (Type=8/0)



- Prüfen der Erreichbarkeit
- Nutzung MS-DOS/UNIX-Kommando ping, z.B.: `ping 194.94.204.23`

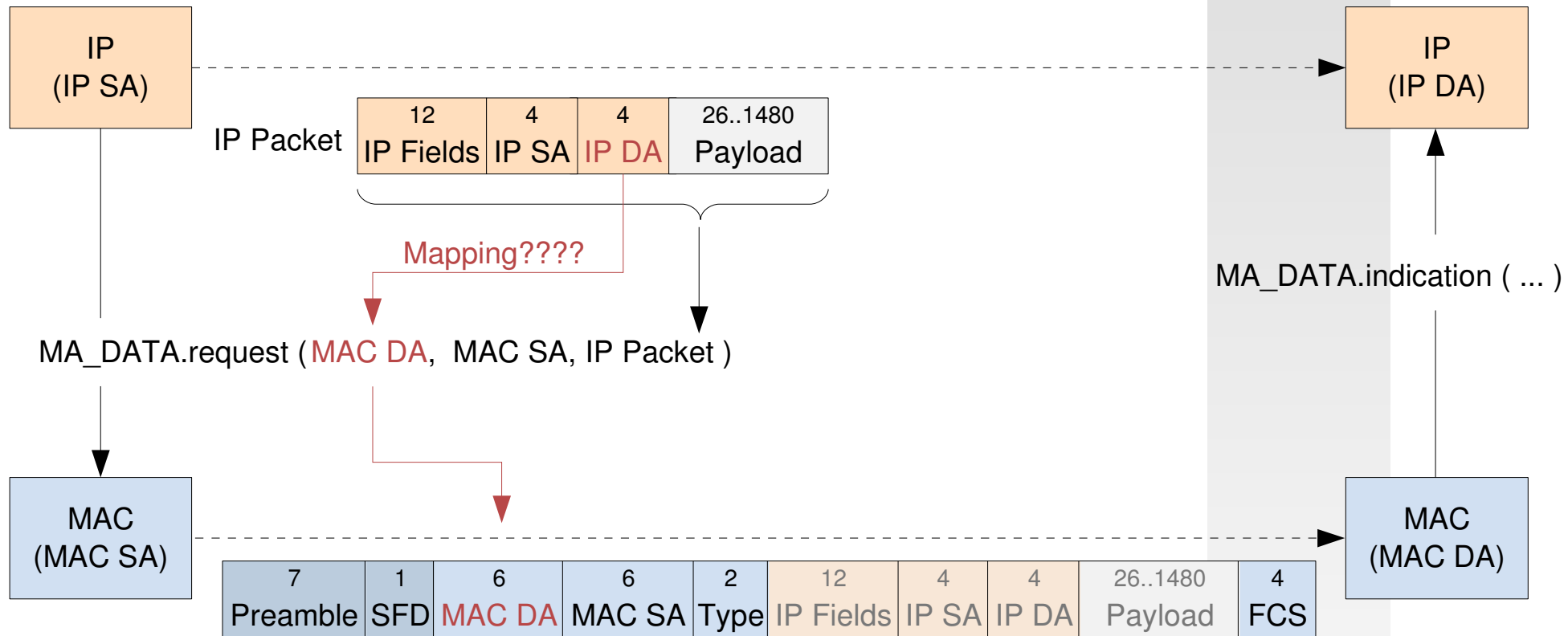
Path MTU Discovery (RFC 1191)

DF = Don't Fragment
TL = Total Length



Type=3 : Destination Unreachable
Code=4: Fragmentation Needed and
DF Flag was Set

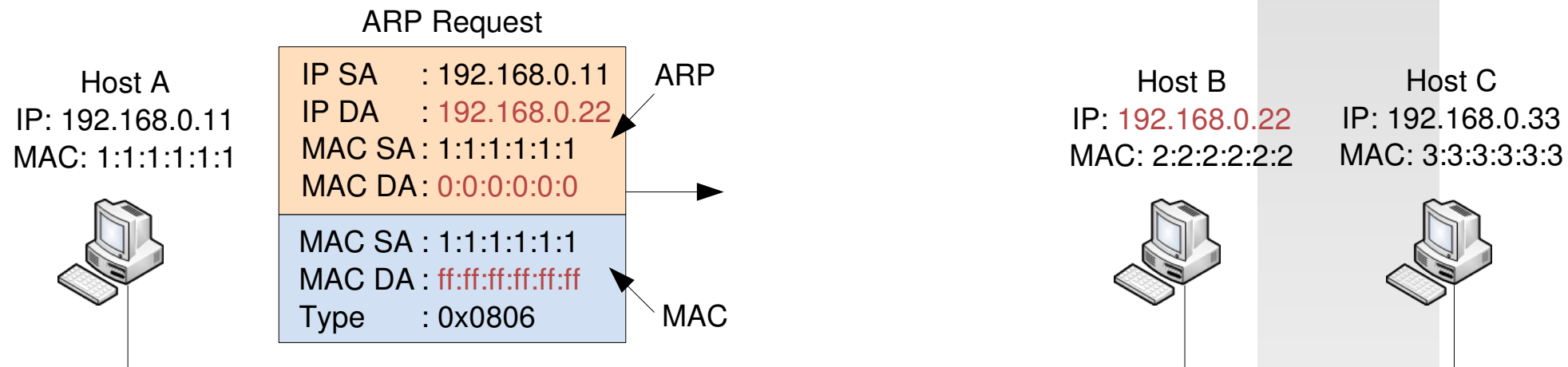
Address Resolution: Problemstellung



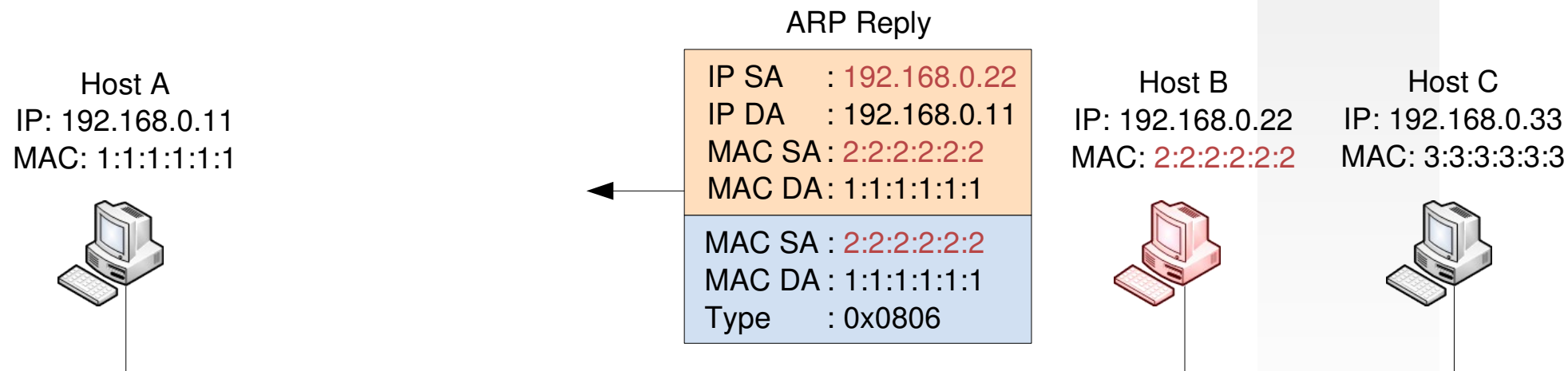
MAC DA MAC Destination Address
 MAC SA MAC Source Address
 IP DA IP Destination Address
 IP SA IP Source Address

LAN Adressierung

Address Resolution Protocol (ARP)



Prinzip des ARP



□ Internet Protokoll

- Network Layer im TCP/IP
- Adressierung
- Wegwahl (Routing)
- Fragmentierung

□ Adressierung

- klassenbasiert mit Subnet-Mask
 - Subnetting (gleichgroße Subnetze)
 - Supernetting
- klassenlos mit Netzwerkpräfix

□ Fragmentierung

- Zerlegung und Zusammensetzen
- entsprechend MTU
- Fragmente unabhängig

□ Routing

- statisch durch manuelle Konfiguration
- dynamisch mittels Protokollen

□ ICMP

- Austausch von Nachrichten
- Fehlermeldungen

□ Automatische Adresszuordnung

- Erstellung von Zuordnungstabellen
IP/MAC-Adressen
- ARP